UNIVERSIDAD NACIONAL DE INGENIERIA

Facultad de Ingeniería Industrial y de Sistemas

PLAN DE CONTINGENCIAS Y DE RECUPERACIÓN DE DESASTRES

INFORME DE INGENIERIA

Para optar el Título Profesional de

INGENIERO INDUSTRIAL

CARLOS AUGUSTO BARRAGAN CHUMPITAZ

LIMA – PERU
2002

INDICE

2. DESCRIPTORES TEMÁTICOS

Se ha considerado los siguientes descriptores temáticos:

- Plan de Contingencias
- Contingencias
- Recuperación de desastres
- Plan de prevención
- Plan de ejecución
- PERUPETRO
- Empresa petrolera
- Empresa supervisora
- Área de Sistemas
- Centro de procesamiento de respaldo
- Escenarios de Contingencias
- Auditoria de Plan de Contingencia
- Sector Hidrocarburos
- Petróleo

3. RESUMEN EJECUTIVO

De acuerdo a los objetivos definidos en el Plan Estratégico de PERUPETRO S.A., es necesario tener información confiable que permita tomar decisiones con menor riesgo en el momento adecuado. De esta estrategia, se desprende que el Área de Sistemas forma parte importante dentro los objetivos a lograr en dicho plan. Así, se hace necesario tener un Plan de Contingencias y de Recuperación de Desastres para el Área de Sistemas que asegure la continuidad de sus procesos críticos.

El presente trabajo tiene por finalidad mantener un plan escrito y explícito de las políticas y normas generales que permitan asegurar la continuidad en los procesos críticos del Área de Sistemas de PERUPETRO S.A., en la eventualidad de una falla mayor de equipos, del software, de las comunicaciones, pérdida de los datos relevantes, destrucción temporal o permanente de las instalaciones, o ausencias prolongadas de personal clave.

Las partes principales en las cuales se encuentra dividido este plan son:

- **Plan de Prevención:** contiene todas las acciones y procedimientos orientados a **prevenir** que ocurra un evento que impida la normal actividad del servicio. Se pone énfasis en la seguridad física, la seguridad del software base y las aplicaciones en uso, los equipos críticos, comunicaciones y la seguridad referida al personal.

- **Plan de Ejecución:** define los escenarios de Contingencias conteniendo las prioridades de reposición por procesos, así

como los procedimientos detallados para **actuar** frente a las contingencias según la fuente de origen de las mismas: pérdida de local e infraestructura, pérdida de equipos computacionales críticos, pérdida de software base y aplicaciones de soporte, pérdida de comunicaciones de voz y datos, pérdida de datos relevantes y de personal clave. Asimismo, define las características mínimas que debe tener un Centro de Procesamiento de Respaldo (CPR) y la organización básica que debe tener éste respecto al personal y equipo.

A partir de la importancia de tener sistemas confiables, podemos apreciar el Gráfico Nro. 1 "Arquitectura de Sistemas Confiables" el mismo que nos muestra las bases en las que se fundamenta los sistemas con esas características, las cuales son:

- Personal clave
- Software aplicativo
- Comunicaciones
- Equipos y software base
- Infraestructura base

Cada uno de estos pilares deberán ser lo suficientemente seguros y confiables de manera que, en conjunto, el sistema también lo sea. Asimismo, el gráfico muestra que la labor no se encuentra específicamente en el Área de Sistemas sino que es una labor compartida con varias áreas de la empresa.

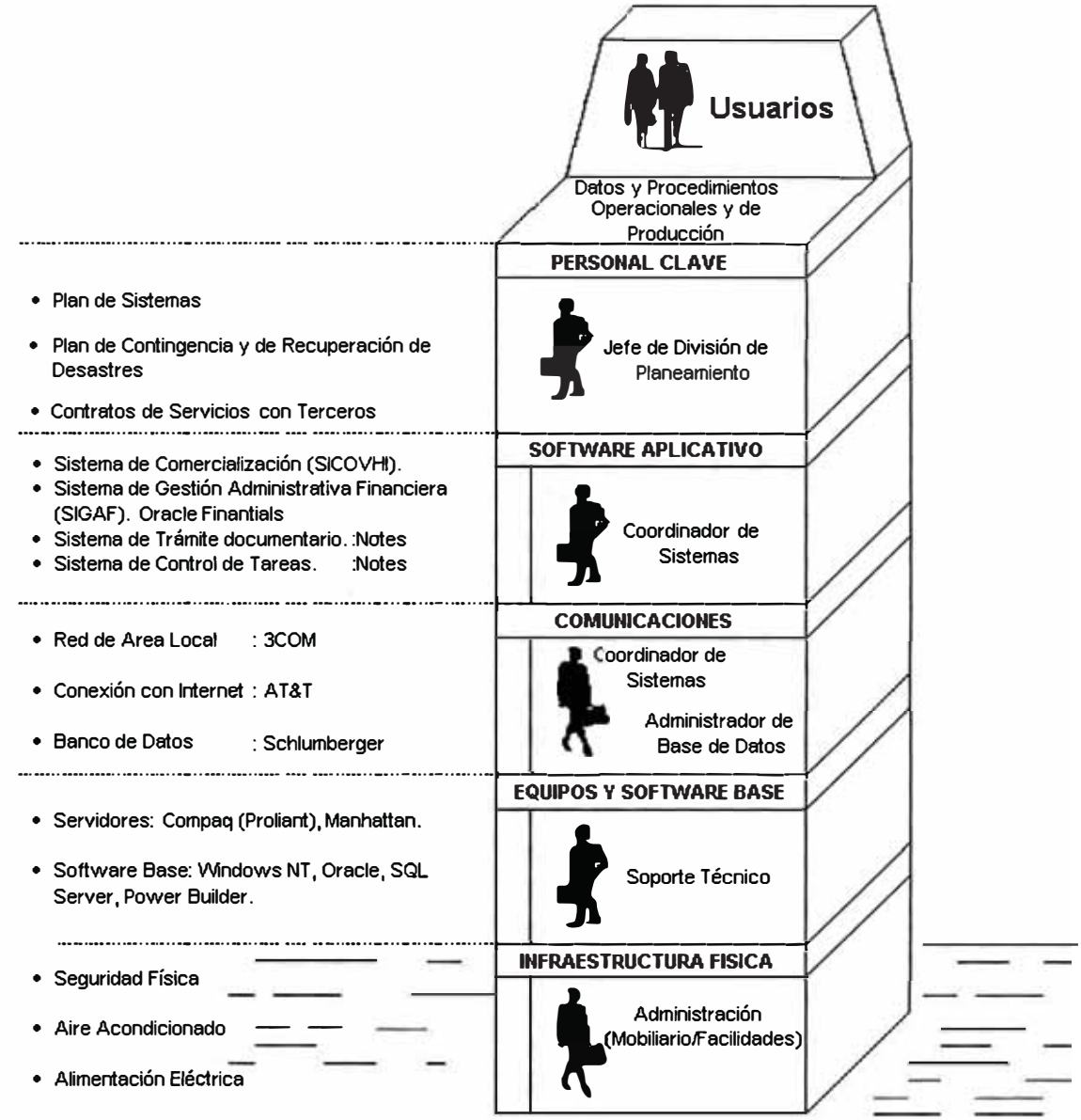


Gráfico Nro. 1 Arquitectura de Sistemas Confiables

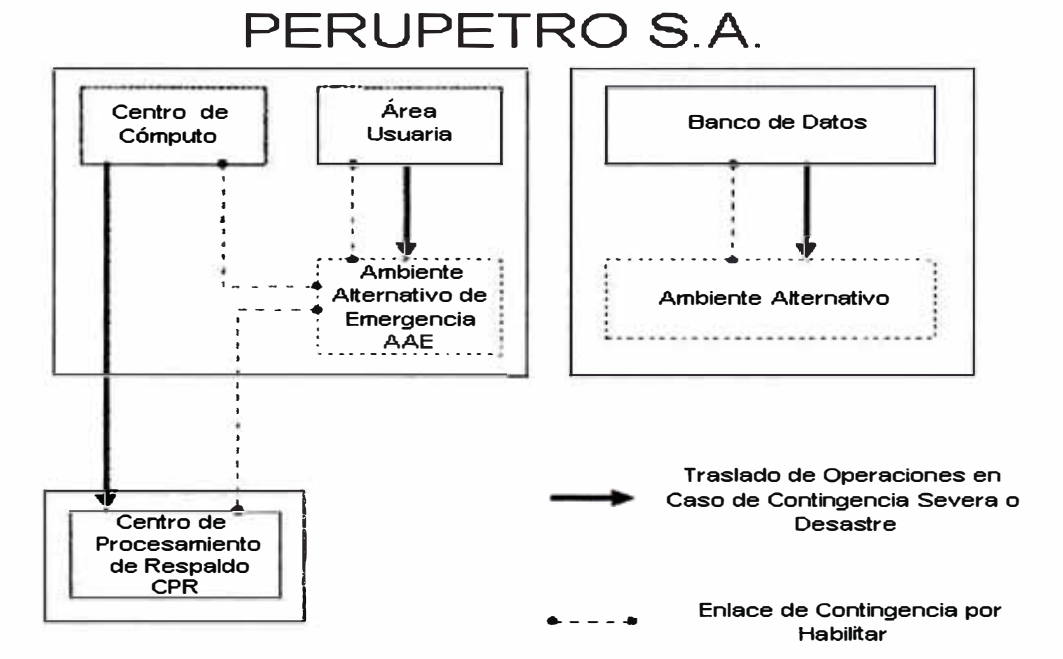
Por otro lado, con el fin de definir los probables escenarios se describen tres (3) áreas de desastres posibles:

- Centro de Cómputo
- Áreas usuarias
- Oficina de Banco de Datos

A continuación, se presenta el cuadro de escenarios posibles y las alternativas de solución propuestos

	Centro de Cómputo	Areas Usuarias	Banco de Datos	Respuesta
Escenario 1	Inhabilitado	Operativa	Operativo	CPR
Escenario 2	Operativo	Inhabilitado	Operativo	Ambiente alternativo de emergencia
Escenario 3	Inhabilitado	Inhabilitado	Operativo	CPR + Ambiente alternativo de emergencia
Escenario 4	Operativo	Operativo	Inhabilitado	Oficina Principal de Schlumberger

El siguiente gráfico nos muestra los movimientos entre el Centro de Procesamiento de Respaldo (CPR), Ambiente Alternativo de Emergencia (AAE)y Ambiente Alternativo (AA) de Banco de Datos cuando se presente una contingencia en PERUPETRO S.A.



Asimismo, se define los equipos necesarios para afrontar una contingencia y las funciones y responsabilidades de cada uno de ellos, logrando una recuperación efectiva, en caso se presente una falla que no permita a la empresa continuar con sus procesos en forma normal. Estos equipos son:

- Equipo de Manejo de Emergencia
- Coordinador del Plan de Contingencias
- Equipo de Apoyo
- Equipo de Soporte Técnico

Dentro de las principales conclusiones obtenidas en la elaboración del presente trabajo podemos mencionar:

- Cualquier sistema o procedimiento que procese información importante y/o sensible, debe tener un Plan de Contingencias que permita continuar su ejecución a pesar de la ocurrencia de un desastre que imposibilite su normal funcionamiento.
- La complejidad y profundidad de un Plan de Contingencias está directamente relacionada a la complejidad del sistema, su costo y su importancia en el cumplimiento de la misión de la organización. Por lo tanto, se debe evitar el "sobre-planeamiento", haciendo que el Plan de Contingencias consista en la descripción de una serie de "acciones" orientadas a la recuperación del sistema.
- Como una regla general, mientras más adverso sea el impacto de un evento (destrucción total del edificio por un terremoto, fuego o inundación) menor es la probabilidad de su ocurrencia.

- Los planes deberán estar escritos y ser de conocimiento de todo el personal apropiado, así como ser probados periódicamente y actualizados según las necesidades si se desea que el plan sea efectivo y cumpla los objetivos trazados en su elaboración.
- El Plan de Contingencias de PERUPETRO S.A. puede ser utilizado por cualquier otra empresa como modelo pues las necesidades del Área de Sistemas se repiten en otras empresas. Será necesario realizar ajustes al Plan para adecuarlo a los requerimientos específicos de cualquier empresa.
- Es necesario proporcionar la importancia debida a las actividades de prevención pues estas, correctamente ejecutadas, disminuyen la probabilidad de ocurrencia de desastres.
- Es necesario probar periódicamente el plan para conocer si los premisas o características principales al elaborarlo continúan vigentes o no. De no ser así, es necesario actualizarlo. Se recomienda una periodicidad de tres (3) meses para realizar las pruebas y de seis (6) para su actualización.
- Cada empresa deberá elaborar un Análisis de Impacto, similar al Anexo Nro. 1 de este informe, para determinar los costos asociados a un desastre cuando se tiene o no un Plan de Contingencias. Asimismo, deberá definir sus procesos y equipos críticos, con el fin de tener claramente definido el plan de prevención o ejecución correcto.

4. INTRODUCCION

Dentro del Plan Estratégico Empresarial de PERUPETRO S.A. se encuentra define la estrategia de brindar sistemas y servicios confiables a sus usuarios.

Un sistema confiable es aquel con el que se puede contar para brindar sus servicios a los usuarios cuando estos lo requieran.

Sin embargo, construir y operar sistemas confiables es un proceso continuo que incluye complejas interdependencias entre los siguientes componentes de una empresa o institución

- Infraestructura Física
- Equipos y Software Base
- Equipos y Servicios de Comunicaciones
- Software Aplicativo
- Datos y Procedimientos Operacionales
- Personal Operativo y Especializado

Adicionalmente, un Plan de Contingencia se desarrolla para proveer la recuperación óptima posible en la eventualidad que ocurra una pérdida de capacidad operativa, una pérdida de datos o se produzca una falla en las medidas de seguridad.

Uno de los beneficios de contar con un Plan de Contingencias es que, al existir un planeamiento de la recuperación del evento o desastre, se evita la pérdida de tiempo valioso que se debe emplear en la recuperación misma.

Todos los sistemas de soporte a las operaciones (redes, sistemas multi-usuarios, servidores, etc.), o cualquier sistema o procedimiento que procese información importante y sensible, debe tener un Plan de Contingencias particular.

La complejidad y profundidad del plan está directamente relacionada a la complejidad del sistema, su costo y su importancia en el cumplimiento de la misión de la organización. Por lo tanto, se debe evitar el "sobre-planeamiento", haciendo que el plan de contingencia consista en la descripción de una serie de "acciones" orientadas a la recuperación del sistema.

Los planes de contingencias no se deben concentrar en eventos límites o desastres, en detrimento del planeamiento de acciones menos catastróficas. Como una regla general, mientras más adverso sea el impacto de un evento (destrucción total del edificio por un terremoto, fuego o inundación) menor es la probabilidad de su ocurrencia.

Dentro de las causas de las caídas de sistemas podemos mencionar:

- Daños en discos duros: Los daños varían en severidad, desde pequeñas fallas que son reparadas con herramientas de software, a graves daños físicos que destruyen el disco en forma permanente. Particiones de disco dañadas o corruptas contribuyen a la pérdida de datos. Hay que tener en cuenta que cualquier dispositivo mecánico eventualmente falla.

- Fallas del Equipo Computacional: Los discos son solamente una parte funcional de una computadora; si otro componente físico falla tal como una tarjeta madre, memoria, tarjeta de red, entre otro dispositivo, el sistema puede estar inoperativo por horas o días. Aunque la información almacenada en discos no está en peligro, para muchas empresas el costo de no poder utilizar el sistema es tan alto como perder datos.

- Fallas en el Software: Software corrupto (generalmente copias piratas que se utilizan ilegalmente en las empresas) o incompatible puede producir una caída en los servidores; hoy en día, los ambientes de los sistemas operativos y aplicaciones críticas son complejas y frecuentemente dependen del proveedor o de elementos de terceras partes; además, según el tipo de ambiente de los sistemas operativos o aplicaciones, las actualizaciones de software, patches (parches), y nuevas versiones pueden tener un efecto inesperado o indeseado.

- Errores de Usuarios o Administradores: Los errores humanos también pueden causar una caída del sistema. Un usuario o administrador puede causar intencionalmente el borrado de archivo de sistemas, archivos de datos o directorios.

- Virus: Los sistemas se pueden poner fuera de servicio, por problemas del sistema operativo causado por un virus. Los virus son una real y potente amenaza para la infraestructura de datos. Los virus que atacan el sector de arranque son más serios que lo que muchas personas creen.

Frecuentemente, el impacto de un virus es sentido cuando el sistema está siendo actualizado y el proceso entero no funciona correctamente. La peor de las realidades, es que Internet y el correo electrónico pueden ser usados para transportar e introducir virus dentro de la red (archivos de texto o planillas de cálculo anexos en los mensajes, que incluyen macros con virus).

Los planes deberán estar escritos y ser de conocimiento de todo el personal apropiado, así como ser probados periódicamente y actualizados según las necesidades si se desea que el plan sea efectivo y cumpla los objetivos trazados en su elaboración.

5. OBJETIVO DEL PLAN

Elaborar un plan escrito y explícito de las políticas y normas generales que permita enfrentar eficientemente la eventualidad de una falla mayor de equipos, del software, de las comunicaciones, pérdida de los datos relevantes, destrucción temporal o permanente de las instalaciones, o ausencias prolongadas de personal clave manteniendo la continuidad de los procesos de PERUPETRO S.A.

6. ALCANCE DEL PLAN

El ámbito de estudio del presente trabajo es el Área de Sistemas de la empresa PERUPETRO S.A.

7. ASPECTOS GENERALES DE LA EMPRESA

Con el fin de entender las particularidades de PERUPETRO S.A., se revisa en esta sección los aspectos generales de la empresa, proporcionando el contexto en que se desenvuelve el Área de Sistema en estudio.

7.1. Visión

PERUPETRO S.A. comparte la visión de ser una "empresa líder en el sector hidrocarburos, de reconocido prestigio en el ámbito nacional e internacional, que concentra sus esfuerzos en posicionar al Perú como un país atractivo a la inversión en actividades de exploración y producción de hidrocarburos, aplicando términos contractuales competitivos".

Además PERUPETRO S.A. busca ser una "empresa reconocida por sus firmes valores de ética, transparencia y honestidad; por contar con personal especializado, que actúa

con dedicación y profesionalismo; y por contribuir al desarrollo sostenible del país".

7.2. Misión

Promover y contratar, en condiciones competitivas y en representación del Estado Peruano, las áreas de filiación hidrocarburífera, con el objetivo de incrementar la producción y reservas de hidrocarburos del país.

También es parte de su misión el "supervisar los contratos para la exploración y explotación de hidrocarburos, verificando el cumplimiento de los términos contractuales, efectuando una eficiente y transparente captación de la renta petrolera, así como, facilitando la ejecución de las actividades establecidas en los Contratos y Convenios de Evaluación Técnica; con el fin de lograr un adecuado desarrollo de la industria hidrocarburífera del país".

Así, PERUPETRO S.A. tiene como objetivo estratégico general el "atraer inversión para las actividades de exploración y explotación de hidrocarburos en el Perú, con el fin de incrementar la producción y reservas de petróleo y gas, tendientes a mejorar la balanza comercial de hidrocarburos del país; así como, desarrollarse empresarialmente según las necesidades de la industria de hidrocarburos y del Estado Peruano".

7.3. Organización Funcional

A continuación se presenta el organigrama de la empresa así como las principales funciones y logros de las áreas más importantes de PERUPETRO S.A.

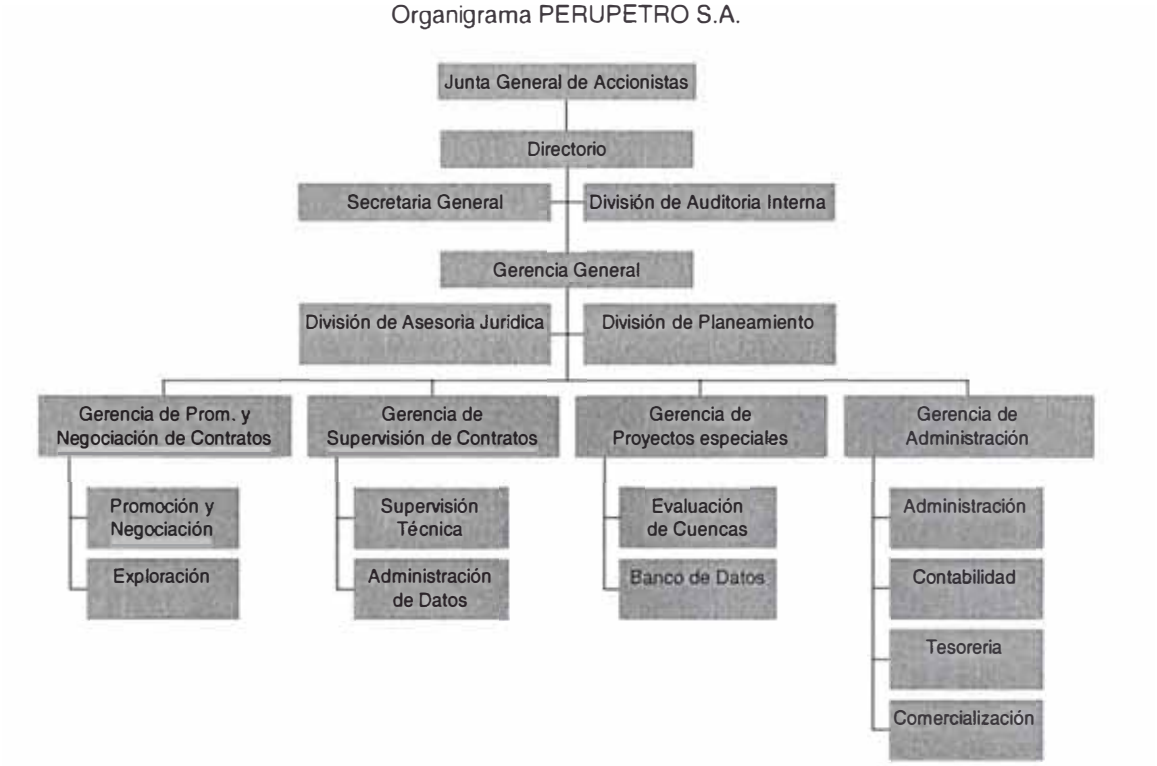


Gráfico Nro. 2 Organigrama de PERUPETRO S.A.

7.3.1. Gerencia de Promoción y Negociación de Contratos

Función:

Esta gerencia se encarga de "la atención de los requerimientos de información técnica de nuevos inversionistas y empresas contratistas, para la evaluación de proyectos de inversión en hidrocarburos".

A partir de septiembre del 2000, la Gerencia de Promoción y Negociación de Contratos está constituida por los Grupos Funcionales "Exploración" y "Promoción y Negociación".

Logros:

El grupo funcional "Negociación de Contratos" cuenta con 46 contratos suscritos desde el inicio de las actividades de PERUPETRO S.A. en Noviembre de 1993. Esta área se encarga de "gestionar la suscripción de las modificaciones a los contratos suscritos con los contratistas". A Diciembre del 2000, "cuenta con 29 contratos vigentes, con un área contratada de 9.45 millones de hectáreas, con 14 de estos contratos en la fase de exploración y 15 en la fase de explotación. La inversión comprometida acumulada es de 1,067 millones de dólares, no incluyéndose la inversión prevista para el proyecto del Gas de Camisea".

7.3.2. Gerencia de Proyectos Especiales

Función:

La Gerencia de Proyectos Especiales "atiende los requerimientos de información técnica de nuevos inversionistas y empresas contratistas interesadas en la evaluación de proyectos de inversión en hidrocarburos". Esta gerencia, a partir de septiembre 2000, quedó constituida por los Grupos Funcionales "Banco de Datos" y "Evaluación de Cuencas".

Logros:

El grupo funcional "Banco de Datos" coordina la escaneo de planos, gráficos y otros, así como la digitalización de curvas de registros eléctricos y mapas. Cuenta con alrededor de 25,000 medios magnéticos, con más de 10,000 documentos codificados y catalogados.

La organización de la base de datos técnicos consta de 4 fases: la fase de organización y mantenimiento del archivo técnico efectuada regularmente; la fase de escaneo de la documentación técnica en la que se ha efectuado el escaneo de 1´078,982 hojas de información técnica histórica y 76,784 hojas de información nueva; la fase de transcripción de cintas, con 24,782 cintas de información sísmica histórica y 10,155 cintas de información reciente; y la fase de modelos de datos de pozos en la que se ha validado información con un avance de 45% y se tiene un avance de 95% en la base de datos documental.

A Diciembre del 2000 "se han codificado e ingresado 1,375 documentos nuevos, completando con lo correspondiente a años anteriores un total de 12,136 documentos codificados, de los cuales se tienen catalogados 11,845 entre informes técnicos, imágenes satélite, archivos de pozo, mapas base, mapas geofísicos, mapas interpretados, secciones estructurales y secciones sísmicas".

7.3.3. Gerencia Supervisión de Contratos

Función:

La Gerencia de Supervisión de Contratos "tiene a su cargo la supervisión de los mismos luego de haber sido suscritos al culminar la etapa de negociación". Para esto, desarrolla sus actividades en dos ámbitos de acción, la supervisión técnica y la supervisión administrativa.

Logros:

Como parte de la Supervisión Técnica de Contratos, durante el año 2000 "se realizaron 191 reuniones de Comités de Supervisión entre los representantes de PERUPETRO S.A. y de los contratistas de los 36 contratos recibidos del año anterior (15 de explotación y 21 de exploración) y de los 2 contratos suscritos (1 de explotación y 1 de exploración). Asimismo se efectuaron un total de 46 viajes de supervisión, en las que se verificaron las principales actividades de Exploración y Explotación realizadas por los contratistas, como cumplimiento de los aspectos contractuales. Asimismo, se efectuaron visitas de supervisión a los respectivos puntos de fiscalización".

Además, "como parte de la Supervisión Administrativa, se ha desarrollado la revisión del factor "R" de diez contratos petroleros, la revisión de las inversiones en exploración efectuadas por Occidental Peruana, sucursal del Perú, los cálculos de compensación económica que deben ser asumidos por Petro-Tech, la

liberación de 24 fianzas que garantizaban programas mínimos de trabajos, gestiones ante aduanas, la revisión de los costos operativos que forman parte de las tarifas de fraccionamiento para determinar la regalía de los líquidos del gas natural del Lote 31-C, entre otras actividades".

"El año 2000 se inició con la supervisión de 36 contratos, a los cuales se incorporó dos más, suscritos durante el año y la unificación de dos contratos en uno solo. Con los ocho contratos terminados a fines del 2000, se encuentran vigentes 29 contratos, con un total de área contratada de 9´452,912 hectáreas. 14 de estos contratos se encuentran en la fase de exploración y 15 en explotación. La inversión comprometida en base a los programas mínimos de trabajo de cada contrato, acumulada a Diciembre 2000, es de US$ 1,315.99 millones de dólares".

Por otra parte la "actividad exploratoria" efectuada en el 2000 "se concentra en la perforación de 5 pozos exploratorios, y el registro de sísmica en el Lote Z-2B con un total de 1,346 Kms de 2-D. Adicionalmente se efectuó 1,105 km2 de sísmica 3-D. Es importante mencionar que la empresa contratista Olympic del Lote XIII efectuó declaración de descubrimiento comercial. Asimismo, el descubrimiento de reservas petrolíferas en el yacimiento Siches del Lote Z-2B. Por otro lado, se continúa desarrollando el estudio de pre-factibilidad para definir la viabilidad de la explotación comercial de los

tres yacimientos: Paiche, Piraña, y Dorado en el Lote 67, los que descubrieron petróleo pesado en el año 1998".

"Durante el año 2000 los contratistas lograron una producción promedio diario de hidrocarburos líquidos fiscalizados a nivel nacional de 99,217 barriles por día, menor en 6,710 BPD (6.34%) respecto del año 1999, debido principalmente a la declinación de los campos. La producción promedio a nivel nacional de gas natural fiscalizado para el año 2000, fue de 33.29 MCPD. Este promedio es menor en 6.83 MCPD (17.02%) con respecto al promedio obtenido en el año 1999, debido principalmente a la menor demanda de gas para el despacho del sector eléctrico".

7.3.4. Gerencia de Administración

Función:

La Gerencia de Administración "como órgano de apoyo, tiene bajo su responsabilidad la gestión de los recursos humanos, materiales, económicos y financieros, así como la comercialización de hidrocarburos de propiedad de la empresa".

Logros*:*

"En el año 2000 la Gerencia de Administración avanzó con el desarrollo de proyectos de importancia estratégica para PERUPETRO S.A.. Uno de dichos proyectos, es el que la empresa cuente con un Sistema Integrado de Gestión Administrativo Financiera SIGAF. Para ello se llevaron adelante las actividades de selección, contratación e inicio de la implantación del

mencionado sistema. En este mismo campo, se concretó la implantación del Sistema de Comercialización de Hidrocarburos líquidos SICOVHI, con el concurso del Agente de Ventas de la empresa, la compañía Glencore AG".

"Respecto a captación y transferencia de la renta petrolera, y como resultado del elevado nivel de los precios internacionales de los hidrocarburos, la empresa cumplió con su importante rol de transferir recursos tanto a las distintas circunscripciones por concepto de canon y sobrecanon por hidrocarburos, por le monto de S/. 407.10 millones de nuevos soles, un 55.7% mayor que el año anterior, como al Tesoro Público, del orden de S/. 486.19 millones de nuevos soles, 70% mayor al año anterior. Es importante destacar en términos de lograr una mayor transparencia y un mejor servicio a las entidades perceptoras del canon y sobrecanon por hidrocarburos, que en el año 2000 la empresa incorporó en su página web, información detallada de los pagos efectuados por ambos conceptos".

"Para efectuar la comercialización de hidrocarburos a través de terceros conforme lo señala la Ley orgánica de Hidrocarburos, la firma Glencore AG, de amplio prestigio internacional, continuó con la función de Agente de Ventas de PERUPETRO S.A."

"En el 2000 los precios internacionales del petróleo crudo mostraron un comportamiento creciente en

relación al año 1999, alcanzando un máximo de 34,3968 US$/Bl en el mes de Noviembre, para el crudo marcador –West Texas Intermediate WTI- utilizado en el 100% de las negociaciones para la venta del Petróleo Crudo Loreto. El valor más bajo fue de 25.7837 US$/Bl durante el mes de Abril. El precio promedio del WTI se incrementó en un 57.41% comparado con el promedio del año 1999".

"El valor FOB del Petróleo Crudo Loreto tuvo un incremento del 69.08% respecto al obtenido en el año 1999. Entre los factores que causaron el incremento en la cotización internacional del Petróleo Crudo Loreto se tienen:

- Reducción de la producción mundial de petróleo crudo acordada por los países integrantes de la OPEC y su estricto cumplimiento durante el año 2000. Como consecuencia de dicha medida, disminuyó la oferta de crudos pesados que compiten con el crudo Loreto.
- Mejores rendimientos económicos de refinación del Petróleo Crudo Loreto en Refinería La Pampilla y Refinería Conchán.
- Esfuerzo desplegado para efectuar ventas a las refinerías con alto grado de conversión ubicadas en Corea del Sur y en Chile, logrando obtener la presencia del Petróleo Crudo Loreto en dichos mercados".

"En el año 2000 se embarcaron en Bayóbar 12.65 millones de barriles de Petróleo Crudo Loreto y se suscribieron 28 contratos de compra-venta de los cuales 11 fueron de exportación y 17 de ellos corresponden a ventas nacionales. Para cumplir con los contratos de compra-venta se efectuaron 10 embarques de exportación y 34 para atender los pedidos locales"

7.3.5. División de Asesoría Jurídica

Función:

La división de Asesoría Jurídica "participa directamente en los procesos de calificación de empresas petroleras y en los de negociación de los contratos de exploración y explotación de hidrocarburos, hasta la culminación del trámite de aprobación de ellos por Decreto Supremo". De igual modo, "apoya constantemente las consultas derivadas de la supervisión de los contratos. Asimismo, es constante y permanente la participación de la Asesoría Jurídica en la revisión y visación de contratos de servicios, de trabajo, de adquisición de bienes, y obras entre otros".

Logros:

La Asesoría Jurídica durante el año 2000, "ha elaborado diferentes propuestas de dispositivos legales vinculados no solo a garantizar, sino también, a incrementar la inversión de riesgo y de largo plazo, en las actividades de exploración, explotación de hidrocarburos, que tienen como objetivo asegurar la competitividad de la contratación y la gestión administrativa".

7.3.6. División de Planeamiento

Función:

La División Planeamiento "cumple la labor de consolidación de la información de la empresa relativa a la formulación del Plan Operativo y Presupuesto, así como de su ejecución". En este sentido durante el año 2000, "ha verificado el cumplimiento de los objetivos de las áreas como aporte a los objetivos de la empresa durante el año 2000 y verificado el cumplimiento de los gastos administrativos dentro de los límites totales del presupuesto".

Logros:

Asimismo, durante el año 2000 "se logró desarrollar con la participación de todas las áreas de la empresa el Plan Estratégico Empresarial 2001-2005, en el cual se resumen las líneas de acción a seguir para el logro del objetivo central de la empresa, que es el incremento de las inversiones en exploración y explotación de hidrocarburos".

7.3.7. División de Auditoria Interna

La División de Auditoria Interna durante el año 2000, "ha desplegado su accionar de control, hacia dos frentes importantes de la empresa: uno de cumplimiento normativo y operativo, verificando la observancia de las normas de gestión y del proceso presupuestal". De otro lado "bajo un enfoque de control técnico, se practicaron

visitas de inspección a los puntos de medición y fiscalización de hidrocarburos de los lotes de explotación en Talara y Selva".

7.4. Diagrama de Procesos Operacionales

A continuación se listan los procesos principales que se han detectado fruto del análisis funcional y de arquitectura de datos realizado en octubre del 2000.

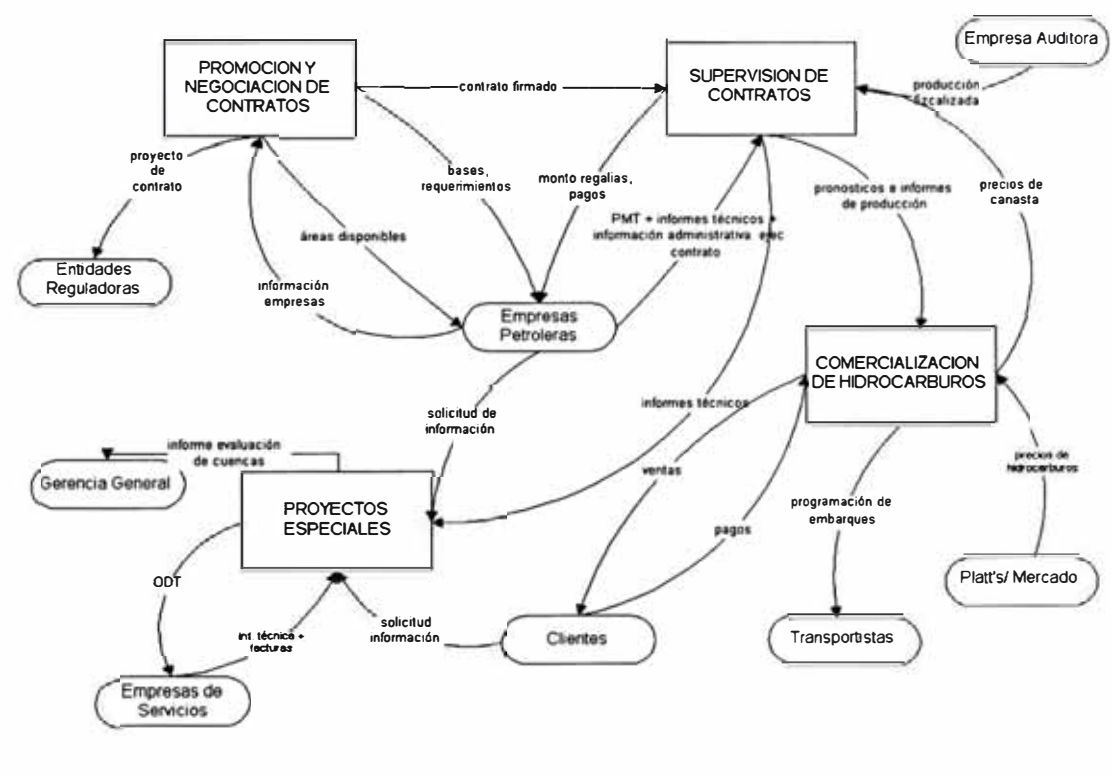


Gráfico Nro. 3 Diagrama Funcional de PERUPETRO S.A.

7.5. Relación de Principales Procesos Operacionales

PROCESOS PRINCIPALES
• Promoción y Negociación de Contratos • Supervisión de Contratos • Comercialización de Hidrocarburos • Proyectos Especiales
PROCESOS DE SOPORTE
• Planeamiento • Logística • Tesorería • Contabilidad • Recursos Humanos • Sistemas • Asesoría Jurídica • Auditoria Interna • Secretaría General

7.6. Descomposición Funcional

A continuación se presentan los procesos principales a cargo de las áreas funcionales de PERUPETRO S.A.

PROCESOS PRINCIPALES
PROMOCIÓN Y NEGOCIACIÓN DE CONTRATOS • Promoción de lotes • Calificación de empresas • Negociación de contratos • Suscripción de contratos
SUPERVISIÓN DE CONTRATOS Técnica • Supervisión contrato de explotación/ exploración • Medición de la producción • Catastro petrolero • Apoyo a entidades internas y externas Administrativa • Cálculo de regalías • Revisión de las cuentas de factor R • Procesamiento de pagos de derechos aduaneros • Supervisión administrativa del contrato • Control de fianzas • Control de pago de aporte de capacitación
COMERCIALIZACIÓN DE HIDROCARBUROS • Programación de Embarques • Ventas • Administración de Precios y Canastas • Elaboración de Pronósticos • Estrategia Comercial • Evaluación de Gestión del Agente de Ventas
PROYECTOS ESPECIALES • Evaluación de Cuencas • Convenios Especulativos • Banco de Datos ✓ Organización de la base de datos ✓ Venta de información técnica ✓ Convenios de evaluación técnica ✓ Administración del archivo técnico
PROCESOS DE SOPORTE
PLANEAMIENTO • Planeamiento Estratégico • Planeamiento Operativo • Presupuesto • Plan de Sistemas • Organización y Métodos • Acciones Seguimiento Auditoria
AUDITORIA INTERNA • Plan Anual de Control • Acciones de Control

• Acciones Periódicas • Hoja de Recomendación
SECRETARÍA GENERAL • Preparación Agendas de Directorio • Preparación Acuerdos de Directorio • Preparación Actas de la Junta General de Accionistas
LOGÍSTICA • Adquisiciones y Contratos • Recepción de Bienes y Servicios • Actualización Catálogo de Proveedores
ADMINISTRACIÓN INTERNA • Administración Passwords de Teléfonos • Control de Llamadas • Correo de Voz
TESORERÍA • Flujo de Caja • Transferencia al Sector Público • Cálculo del Canon • Obligaciones Recurrentes • Control Fianzas • Control Bancario
CONTABILIDAD • Registro Contable • Emisión de Estados Financieros • Emisión de Reportes de Gastos por Centros de Costo
RECURSOS HUMANOS • Selección de Personal • Capacitación • Asistencia Social • Planillas • Evaluación de Personal
SISTEMAS • Mantenimiento de Hardware • Respaldo de Información • Soporte a Usuarios y Aplicaciones • Proyectos • Administración Red y Software Base • Actualización de La Página Web
ASESORÍA JURÍDICA • Análisis y Proyección de Dispositivos • Asesoría Legal Interna • Análisis Comparativo de la Legislación Internacional • Tratamiento de las Comunidades Nativas

7.7. Identificación de los usuarios afectados

A continuación se presentan los principales usuarios de PERUPETRO S.A. que serían afectados por una contingencia:

Área	Usuario	Ubicación
Presidencia de Directorio	• Presidente de Directorio • Secretaria Presidencia de Directorio	Oficina Principal de PERUPETRO S.A.
Gerencia General	• Gerente General • Secretaria Gerencia General	Oficina Principal de PERUPETRO S.A.
Gerencia Supervisión Contratos	• Gerente Supervisión Contratos • Secretaria Supervisión Contratos • Coordinador de Contratos • Coordinador Técnico I • Coordinador Técnico II • Supervisor Administración Contratos • Supervisora de Contratos	Oficina Principal de PERUPETRO S.A.
Gerencia de Negociación Contratos	• Gerente Negociación Contratos • Secretaria NEC • Coordinador NEC • Supervisor	Oficina Principal de PERUPETRO S.A.
Gerencia de Proyectos Especiales	• Gerente de Proyectos Especiales. • Coordinador del Banco de Datos.	
Gerencia de Administración	• Gerente Administración • Secretaria de Administración • Secretaria Recepcionista • Auxiliar II • Administrador General • Secretaria III • Supervisor de Personal • Contador General • Sub-Contador • Supervisora Contabilidad • Tesorero • Asistente de Tesorería • Coordinador Comercial	Oficina Principal de PERUPETRO S.A.
División de Asesoría Jurídica	• Jefe de Asesoría Jurídica • Secretaria de Asesoría Jurídica • Supervisor III • Asesor Legal	Oficina Principal de PERUPETRO S.A.
División Auditoria Interna	• Auditor Interno • Secretaria Auditoria Interna	Oficina Principal de PERUPETRO S.A.
Planeamiento	• Jefe División Planeamiento • Coordinador de Sistemas	Oficina Principal de PERUPETRO S.A.

8. PLAN DE PREVENCION

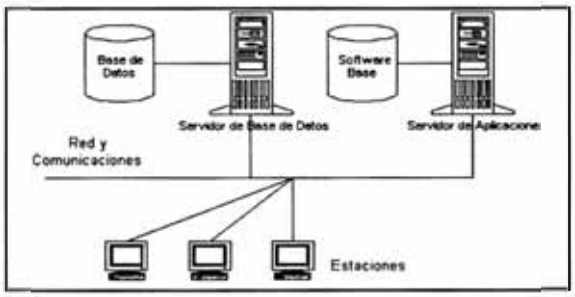
El Plan de Prevención tiene por finalidad establecer los procedimientos que permitan disminuir las posibilidades de que ocurran contingencias que afecten el normal funcionamiento de los sistemas de PERUPETRO S.A.

Los elementos que conforman el Plan de Prevención, tal como se muestra en el Gráfico Nro. 4, son los relativos a :

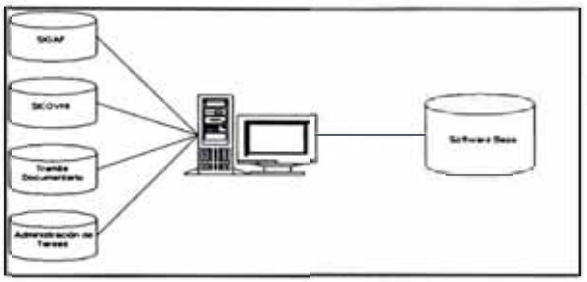
- La Seguridad física
- El Software Base y Aplicaciones
- Los Equipos Críticos
- Las Comunicaciones
- El Personal

Finalmente, se ha elaborado el Anexo Nro. 1 "Análisis de Impacto Económico" de los procesos principales desarrollados en PERUPETRO S.A., el cual nos proporciona una estimación de lo que perdería o dejaría de ganar PERUPETRO S.A., en caso no pueda ejecutar dichos procesos con el recurso humano y material necesario. Asimismo, en este anexo incluimos experiencias pasadas y de consultores en las cuales se estima la pérdida económica por no haber tenido un Plan de Contingencias en el momento oportuno.

Equipos Críticos

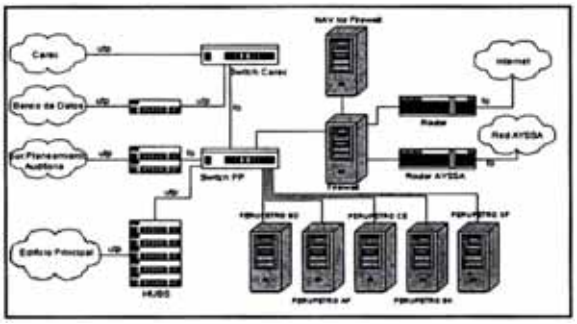


Software Base y



Personal

Comunicaciones



Datos y

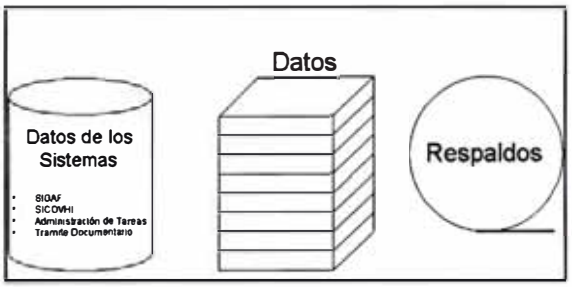


Gráfico Nro. 4 Elementos del Plan de prevención

8.1. Prevención Relativa a la Seguridad Física

Los requerimientos sobre seguridad física comprenden un conjunto de medidas para asegurar áreas, controlar perímetros, controlar las entradas físicas e implantar equipamientos de protección contra robos, incendios, falta de suministro eléctrico, problemas de temperatura entre otros.

A continuación describiremos los aspectos de seguridad física que PERUPETRO S.A. contemplará como parte de su operación diaria.

8.1.1. Seguridad de Ambientes

PERUPETRO S.A. establecerá medidas de seguridad para el ambiente global de trabajo, para el ambiente asignado al centro de cómputo (donde estarán ubicados los servidores, consolas, equipos de comunicaciones, impresoras) y para el ambiente asignado al archivo donde se almacenará toda la documentación relevante de PERUPETRO S.A.

Estos ambientes estarán protegidos por un perímetro de seguridad definido, con controles de entrada apropiados para reducir el riesgo de accesos no autorizados o de daños a los equipos, cintas, documentos y datos.

Cada nivel de protección física tendrá una seguridad perimetral o seguridad física del ambiente definido, alrededor del cual se mantiene un nivel constante de protección. La seguridad perimetral se basará en

parámetros definidos por el Gerente de Administración en coordinación con el Jefe de la División de Planeamiento. Los requerimientos y situación de cada barrera de seguridad dependerán sobre todo del valor de los activos y servicios que deben protegerse.

Se tendrá en consideración las siguientes normas:

- Los equipos computacionales y de comunicaciones (por ejemplo servidores, switchs, hubs, etc.) estarán ubicados en áreas seguras o destinadas a información sensible donde existan riesgos mínimos de accesos no autorizados.

- Se instalarán tabiquerías para separar los diferentes ambientes con diferentes requerimientos de seguridad y prevenir entradas no autorizadas o contaminación del ambiente definido para el centro de cómputo.

- El equipo de servidores centrales estará alojado en áreas dedicadas (centro de cómputo acondicionado) con un ambiente de temperatura y controles de seguridad apropiados.

- El personal del contratista de mantenimiento sólo accederá a las áreas seguras cuando sea requerido y autorizado. Aún con acceso

autorizado deben restringirse sus accesos y controlarse sus actividades (especialmente en zonas de datos sensibles).

- Vigilancia para el control de acceso al ambiente global de trabajo.

8.1.2. Controles Físicos de Seguridad

Existirán controles apropiados de entrada en cada "área de seguridad", que sólo permitan el acceso al personal autorizado, con estas condiciones:

- Los accesos a estas áreas se autorizarán sólo para propósitos específicos y controlados, registrando los datos y tiempos de entrada y salida. Esta medida se aplicará esencialmente para el área destinada al centro de cómputo y al archivo de documentos.

- Se pedirá a todo el personal que lleve una identificación visible dentro del área segura y que observe e informe de la presencia de personal extraño al área.

- Los derechos de acceso se revocarán inmediatamente al personal que deje de laborar o sea asignado a otra área de la empresa.

- El área donde se ubica el Centro de Cómputo, el cual soporta las actividades críticas para el funcionamiento del sistema requerirán un alto nivel de protección física. La selección y diseño de su ubicación tendrá en cuenta la posibilidad de impactos por fuego, inundaciones, explosiones, disturbios y otras formas de desastres naturales o intervenciones humanas.

Se tomarán las siguientes medidas:

- Los servicios críticos se situarán lejos de áreas de acceso público.

- Los materiales combustibles deben almacenarse a una distancia de seguridad del emplazamiento de los equipos de cómputo. Por ejemplo los suministros informáticos como el papel no se almacenarán en la sala de computo.

- Una copia de los datos de respaldo (backup) se ubicarán en un sitio diferente del centro de cómputo y a una distancia conveniente de seguridad.

- El equipamiento alternativo (de respaldo) y la segunda copia de los datos de respaldo (backup) se ubicarán en el local asignado para

el Centro de Procesamiento de Respaldo (CPR).

- Se instalará en el área asignada al centro de cómputo y archivo de documentos, equipamiento apropiado de seguridad: aire acondicionado, detectores de calor y humo, así como medidores de temperatura y humedad. Este equipamiento debe revisarse regularmente de acuerdo con las instrucciones de los fabricantes. Los encargados del centro de cómputo estarán entrenados en su uso adecuado.

- En cuanto a los extinguidores, se colocará uno por cada ambiente definido, con la capacidad adecuada, fácil acceso, peso y tipo de producto adecuado (polvo seco). Se realizará periódicamente la recarga de los extinguidores.

8.1.3. Seguridad del Equipamiento

Para prevenir pérdidas, daños o riesgos de los activos o interrupción del servicio del Sistema, el equipamiento estará físicamente protegido de amenazas y riesgos del entorno. Adicionalmente, el mantenimiento regular del Hardware y Software provee una protección contra fallas del equipamiento.

El mantenimiento preventivo se deberá realizar mínimo 2 veces al año.

Para garantizar la seguridad de los equipos, se tendrá en cuenta la protección contra riesgos de acceso no autorizados a las instalaciones de acometida de energía y sus equipos, así como los sistemas de alimentación ininterrumpida.

A continuación, las características básicas que debe cumplir la seguridad en cuanto a equipamiento:

- ✓ **Instalación y protección del equipamiento**

  El equipamiento se situará en zonas protegidas para reducir el riesgo de daños por las amenazas del entorno, interferencias y oportunidad de accesos no autorizados.

  Se aplicarán estas medidas (considerando la proximidad vertical y horizontal de los riesgos):

  - Los equipos se ubicarán en lugares donde se minimicen los accesos innecesarios a las áreas de trabajo. Las estaciones que manejen información y datos sensibles se ubicarán en lugares donde se reduzca el riesgo de que aquellos estén a la vista.

  - Se identificarán y protegerán estas áreas de amenazas potenciales como fuego, humos,

agua, polvo, vibraciones, agentes químicos o radiaciones electromagnéticas. Se prohibirá fumar y comer en área de servidores. Se tendrá especial cuidado con los materiales más peligrosos que son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

- Se contará obligatoriamente con aire acondicionado en el área asignada a los servidores centrales (centro de cómputo) para mantenerlos a temperaturas recomendadas por los fabricantes.

- Se contará con un ambiente hermético necesario para evitar la contaminación por polvo

✓ **Seguridad al restaurar el equipo**

Cuando ocurra una contingencia, se buscará conocer al detalle el motivo que la originó y el daño causado, lo que permitirá recuperar en el menor tiempo posible el proceso perdido y así asegurar la continuidad del servicio, también se analizará el impacto futuro en el funcionamiento del servicio y así prevenir cualquier implicación negativa.

Las acciones de recuperación disponibles a nivel operativo serán las siguientes:

- Con las copias de respaldo disponibles de los archivos se recuperará el proceso a partir de una fecha determinada.

- Hacer efectivo el procedimiento y cambiar el proceso normal por un proceso alterno de emergencia.

- Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Se tendrá en consideración:

- La existencia de procedimientos relativos a la restauración (a cargo de la División de Planeamiento y Gerencias usuarias).

- Los encargados del centro de cómputo contarán con documentación en donde se guarden las instrucciones actualizadas para el manejo de restauraciones.

✓ **Suministro Eléctrico**

Los equipos deben estar protegidos contra interrupciones del fluido eléctrico u otras anomalías eléctricas.

Debe garantizarse un suministro eléctrico adecuado que cumpla con las especificaciones de los fabricantes de equipos. [1]

- ✓ **Mantenimiento de equipos**

  Los equipos informáticos recibirán mantenimiento preventivo adecuado para asegurar la disponibilidad e integridad de los sistemas de información. Este mantenimiento preventivo se efectuará como mínimo dos (2) veces por año. En particular:

  - Los equipos se mantendrán de acuerdo a las recomendaciones y especificaciones de los fabricantes.

  - Los equipos sólo serán retirados fuera de las áreas para su reparación y servicio por personal del contratista de mantenimiento debidamente autorizado.

  - Se contemplará políticas de mantenimiento preventivo y correctivo de los equipos informáticos, principalmente de los servidores centrales y equipos de comunicación a fin de prevenir posibles fallas en los mismos.

[1] Los servidores centrales cuentan con UPS que asegura su funcionamiento ininterrumpido por lo menos durante **media hora** en caso ocurra un fallo eléctrico.

- Se registrarán documentalmente todos los fallos o sospechas de fallas identificados para la elaboración de estadísticas.

✓ **Control de movimiento de equipos y otros materiales**

El equipo asignado al servicio no se retirará fuera de éste por el personal del contratista de mantenimiento sin la correspondiente autorización por parte de la PERUPETRO S.A.

En caso de ser necesario el movimiento de algún equipo, y previa autorización de PERUPETRO S.A., se registrarán todos los datos necesarios para su control y seguimiento (fecha de salida, motivo de salida, persona que autoriza la salida, lugar de destino, fecha estimada de retorno, etc.)

Los dispositivos de almacenamiento (por ejemplo un disco duro) que contengan datos sensibles y hayan sufrido daños, requieren una minuciosa valoración de riesgos para determinar si deben ser destruidos, reparados o descartados.

8.2. Prevención Relativa a la seguridad del software base y aplicaciones

La información de la empresa constituye uno de los recursos de mayor importancia para PERUPETRO S.A., por ello, se establecen controles a través de este plan para asegurar la

confiabilidad, integridad y confidencialidad de dicha información.

8.2.1. Necesidad de Respaldo

Las copias de respaldo ayudan a recuperar o restaurar la información ante la pérdida de datos generados por: altas o bajas en la fuente eléctrica, electricidad estática, desastres naturales, simples accidentes, sabotaje, falla de los equipos, virus, errores cometidos por los usuarios del sistema de información u otra contingencia que implique pérdida de información o fallas en el equipamiento.

Al momento de desarrollar una estrategia de respaldo de la información, se considera a ésta como una herramienta de gestión muy valiosa que permitirá disminuir potenciales pérdidas de datos, tiempo y dinero que puedan ocasionar interrupciones en los servicios que prestan los sistemas de información.

PERUPETRO S.A. tendrá en cuenta que un respaldo (backup) hecho sin ningún reporte de error no significa que fue resguardado correctamente. Las restauraciones parciales deben realizarse al menos una vez al mes.

- ✓ **Tipos de Respaldo**

  Los tipos de copias de respaldo son clasificados por su estado en la red, cuando la copia se está realizando en línea (on-line) o fuera de línea (off-line), por la cantidad de datos a respaldar: respaldo

completo y parcial; por la forma de respaldar: diferencial, incremental o definido por el usuario.

De acuerdo a la información contenida en la copia de respaldo podemos clasificarlas en:

a) Software Base (Sistema Operativo y Utilitarios)

Busca la prevención de las configuraciones iniciales del sistema con la finalidad de responder ante cualquier tipo de deterioro o falla del sistema operativo y sus utilitarios; como un medio de asegurar el correcto funcionamiento de los equipos y también la performance de los servicios que se brindan.

b) Base de Datos

El objetivo principal de PERUPETRO S.A. es salvaguardar la información contenida en la base de datos; este tipo de copia de seguridad es la que recibe más rigor en su cumplimiento porque la información es considerada como un activo. Dependerá de que esta información esté disponible para que los demás componentes de los sistemas de información realicen su tarea adecuadamente.

c) Aplicaciones

Tiene por objetivo la manutención de copias de archivos fuentes que contienen las aplicaciones de los sistemas de información; para

salvaguardar los sistemas de información y servir como fuente única de información para el desarrollo de aplicaciones, asegurando que la última copia de seguridad tendrá los programas que están actualmente en producción. Por tanto, esta copia debe estar sincronizada con el Coordinador de Sistemas para que cualquier cambio en las aplicaciones tenga copia de seguridad.

d) Otras copias de Respaldo

En este punto tomaremos algunos tipos de copias de seguridad que son eventuales dentro de la operatividad de los sistemas, pero son de real importancia para poder asegurar la continuidad de la disponibilidad de los recursos de los sistemas. Estos tipos de copias de seguridad buscan asegurar las configuraciones de la base de datos que se hayan realizado en el servidor con la finalidad de poder replicar el mismo ambiente y configuraciones en otras instalaciones diferentes. Este, como el resto de copias de seguridad, es de fundamental importancia para el plan de contingencia porque se constituye en el punto de partida para dicho plan.

Asimismo, las copias de respaldo pueden clasificarse por la cantidad de información que ellos contiene, los cuales son:

- ✓ **Respaldo completo**

En donde se respaldan todos los datos, sin discriminación alguna y se efectuará semanalmente.

- ✓ **Respaldo incremental**

En este caso, se hace el respaldo de todos los archivos modificados, desde el último respaldo COMPLETO, y se efectuará diariamente.

- ✓ **Respaldo diferencial**

Es una copia de respaldo de todos los archivos, en tiempos diferentes y conservándolos en el Tape Back-up. Se efectuará de la copia de respaldo del archivo de identificarse puntualmente una necesidad en la que aplique este tipo de respaldo.

- ✓ **Respaldo personalizado**

Sólo respalda los archivos que se especifiquen, se efectuará cuando alguna persona autorizada así lo solicite.

- ✓ **Proceso de Respaldo**

a) Respaldo de Software Base

La copia de respaldo del software base al buscar asegurar las configuraciones del sistema operativo y sus utilitarios, es una copia de respaldo que debe ser obtenida off-line, de manera completa.

El método para obtener estas copias de seguridad será emplear los utilitarios propios del sistema operativo y asegurar de esta forma la disponibilidad de las mismas.

b) Respaldo de Base de Datos

Es la copia de respaldo que recibe mayor rigor. En ésta se realizan copias de la información o de los registros con la finalidad de asegurar la información mantenida en la base de datos.

La copia de seguridad de la información es un proceso diario, en donde se busca asegurar la integridad de la información. También se obtienen copias de seguridad de la base de datos de acuerdo a requerimientos antes o después de un determinado proceso.

Esta copia de respaldo será del tipo de copia definido por el usuario, estructurado modularmente de acuerdo a la funcionalidad de los sistemas, de la información y al tamaño de las tablas, lo cual permitirá un manejo de archivos de respaldo pequeños, y por lo tanto reducir los tiempos de los procesos de las copias de respaldo y de recuperación, sobretodo tener al sistema fuera de línea el menor tiempo posible.

c) Respaldo de Aplicaciones

El respaldo de las aplicaciones busca asegurar que las mismas que actualmente se están utilizando, estén seguras, no se pierdan o deterioren. Esta copia de respaldo será obtenida off-line y de manera completa, buscando asegurar la integridad del sistema.

Las copias de seguridad de las aplicaciones serán obtenidas sincronizando con el área de sistemas las modificaciones realizadas sobre éstas, buscando siempre asegurar que la última copia de seguridad contenga las aplicaciones que están en producción.

d) Otras copias de Seguridad

Dentro de los procesos eventuales de tener copias de seguridad, existen muchas que no son frecuentes, pero son de igual importancia. Estas copias de seguridad buscan asegurar los diseños y configuraciones de la bases de datos principalmente. Dentro de este proceso de copias de respaldo encontramos algunas como:

- Respaldo de los objetos y estructuras de base de datos.
- Respaldo de los privilegios de base de datos
- Respaldo de los archivos de control, entre otros.

Estas copias de seguridad permiten reconstruir todas las configuraciones y ambientes en nuevas instalaciones, además de ser el punto de partida para el proceso de contingencia.

La periodicidad de este tipo de copia de seguridad está establecida de acuerdo a los cambios que se den en las configuración del software, estructuras, privilegios, etc.

- ✓ **Plan de respaldo**

a) Respaldos en medios magnéticos

Uno de los aspectos de mayor relevancia con respecto a la seguridad de los sistemas de información es la existencia de copias de respaldo de la información (backup) que permitan su restauración inmediata ante cualquier eventualidad y aseguren la continuidad de las operaciones. Por tanto, se indica de manera general que:

- PERUPETRO S.A. realizará backups en tapes conteniendo los archivos vitales del Sistema, con la frecuencia y alcances que se señalan en esta sección.

- Adicionalmente, PERUPETRO S.A. mantendrá copia del Sistema Operativo y de la Base de Datos en disco, tanto

en el local principal de operación como en el Centro de Procesamiento de Respaldo. Esto para garantizar un mejor tiempo de restauración en caso de una contingencia mayor.

- PERUPETRO mantendrá copias de respaldo de los sistemas y de la base de datos, tanto en sus oficinas, como en el área de almacenamiento alternativo (Backup-site).

b) Periodicidad del Plan del Respaldo

El respaldo de la información de los Sistemas o aplicaciones se hará de acuerdo a la siguiente frecuencia:

Diario: Se respalda todos los archivos modificados durante el día, después de la finalización de la jornada (procurando que no existan usuarios trabajando con las aplicaciones).

Semanal: Se realiza un respaldo total, después de finalizar la última jornada de la semana.

Mensual: Se realiza un respaldo completo en la última jornada, de la semana restante del mes.

Procesos Especiales Se hace un respaldo completo, cada vez que se cambie la configuración, se actualice el servidor con una nueva versión, se modifiquen aplicaciones o se realicen grandes cambios en el servicio.

Anual : Se realiza un respaldo completo de la base de datos, programas, fuentes y objetos en la última jornada del Año.

El siguiente cuadro muestra las características básicas de las copias de respaldo según su frecuencia.

Frecuencia de Backup	Contenido	Día de Entrega	Periodo de Retención	Cantidad de Copias	Destino
Diario	Base de Datos, Servidores, Estaciones	Martes a Viernes	Una Semana	02	Uno para PERUPETRO S.A. y otra para el (BACKUP Site)
Semanal	Programas Fuentes de los Sistemas, Servidores, Estaciones	Lunes	Un Mes	02	Uno para PERUPETRO S.A. y otra para el (BACKUP Site)
Mensual	Base de datos al cierre de la emisión . Programas fuentes y objetos. Servidores, Estaciones.	Primer día útil del mes	Un Año	01	PERUPETRO S.A.
Anual	Base de datos al cierre del año. Programas fuentes y objetos. Servidores, Estaciones.	Primer día útil del siguiente año	Tres Años	01	PERUPETRO S.A.

Cuadro Nro. 1 Frecuencia y Contenido de las Copias de Respaldo

- ✓ **Procedimientos del Plan de respaldo**

PERUPETRO S.A. deberá designar un lugar seguro para el almacenamiento de todas las copias de respaldo a fin de evitar robos o daños mayores que impidan una reconstrucción exitosa ante una eventualidad.

Una copia de los backups diario y semanal deberán ser almacenadas por la persona responsable de realizarlas en el lugar asignado para tal fin.

Asimismo, las copias de fin de mes, fin de año e histórica deberán ser almacenadas en el lugar asignado para tal fin.

- ✓ **Pruebas de fiabilidad del Plan de Respaldo**

  Se coordinará con el área de sistemas la realización en forma aleatoria de pruebas de restitución completa de algún archivo o directorio en particular, para verificar que el respaldo se está efectuando correctamente. Este procedimiento se debe ejecutar por lo menos de manera mensual y sus resultados deben ser continuamente informados a los responsables de la División de Planeamiento de PERUPETRO S.A. que está a cargo del servicio.

- ✓ **Fiabilidad del Plan de respaldo**

  La fiabilidad de las copias de respaldo deberán ser altas, de esta manera, una copia adicional de los respaldos semanales, mensuales y anuales deberán almacenarse en un lugar seguro fuera de

la empresa. Esta redundancia le otorgará mayor fiabilidad al proceso de restauración de la información requerida.

- ✓ **Almacenamiento de las cintas**

  Es de vital importancia el lugar dónde almacenar las cintas de backup como el backup en sí mismo. Cuando hay una contingencia se debe poder acceder a las cintas rápidamente para reducir los tiempos de para de los sistemas para lo cual PERUPETRO S.A. deberá acondicionar un área destinada al almacenamiento adecuado de los backups (Cintoteca) .

8.2.2. Cambios y Modificaciones al Sistema

Cuando se realicen modificaciones o correcciones a los programas y/o archivos de los Sistemas se tendrán en cuenta las siguientes precauciones:

- Las correcciones de programas deben ser debidamente autorizadas y probadas por PERUPETRO S.A. a través de procedimientos definidos. Con esto se busca evitar que se cambien a una nueva versión que antes no ha sido perfectamente probada y actualizada. Asimismo, se debe actualizar las copias de seguridad de los programas con el fin de contar siempre con la última versión de los programas que se encuentren en producción.

- Los nuevos sistemas deben estar adecuadamente documentados y probados.

- Los errores corregidos deben estar adecuadamente documentados y las correcciones autorizadas y verificadas.

- Los archivos de nuevos registros o correcciones ya existentes deben estar documentados y verificados antes de obtener reportes.

8.2.3. Control de Acceso a los Sistemas de Información

Con el objetivo de prevenir accesos no autorizados a los sistemas, se empezará por definir que el control de acceso a los activos, servicios o datos de los sistemas de información debe responder a los requerimientos del funcionamiento del servicio establecidos por PERUPETRO S.A.

✓ **Derechos de Acceso a Sistemas**

Los derechos de acceso de los usuarios a los sistemas (***perfiles de usuarios***) deben darse según las funciones y puesto de trabajo de los mismos. Para ello se contemplarán los siguientes puntos:

- Mantener actualizado el registro formal de todas las personas con derechos de acceso al servicio, revisándolo de forma periódica para localizar y

eliminar identificadores de usuarios redundantes (duplicados) o sobrantes (no utilizados).

- Eliminar de forma inmediata las autorizaciones de acceso a los usuarios que dejen la organización o cambien su función dentro de ella y comprobar que los identificadores eliminados no sean reasignados a otros usuarios.

- Identificar los privilegios asociados a cada subsistema (el sistema operativo, el gestor de base de datos, etc.) y a cada categoría de empleados que los necesitan.

Este procedimiento debe cubrir desde el momento de dar de alta a nuevos usuarios y su registro para permitir su acceso a activos determinados del Sistema de Información, hasta la formalización de su baja.

✓ **Revisión de los derechos de acceso de usuarios**

Para lograr una protección efectiva del sistema, se necesita la cooperación de los usuarios autorizados. Estos deben saber su responsabilidad en el mantenimiento de la eficacia de los controles de acceso (sus contraseñas, claves secretas de acceso o passwords).

Para mantener un control efectivo del acceso, se propone establecer un ***proceso formal de revisión periódica de los derechos de acceso*** de los usuarios que obligue a:

- Revisar la capacidad de acceso de los usuarios (revisión recomendada cada seis meses).
- Someter a revisión más frecuente los accesos privilegiados (cada tres meses).
- Comprobar regularmente las asignaciones de accesos privilegiados para asegurarse de que éstos no han dado lugar a accesos no autorizados.

✓ **Uso de las contraseñas de acceso**

Las contraseñas son el mecanismo de salvaguarda principal para validar las autorizaciones de acceso a los servicios de los sistemas de información. Todos los usuarios deben conocer y aplicar ciertas reglas para la selección, uso y gestión correctos de sus contraseñas, como:

- Cambiar la contraseña temporal dada por la Administración de seguridad la primera vez que se

acceda al sistema y autoasignarse una contraseña individual.

- Evitar contraseñas deducibles de:
  a) Fechas o series regulares (planetas, días de la semana, meses).
  b) Nombres de la familia, direcciones, teléfonos, placas de auto.
  c) Nombres de la Organización, productos comerciales y similares.
  d) Identificador de usuario, de grupo u otros identificadores de sistema
  e) Números o letras únicamente, o repetición de caracteres seguidos.

- Cambiar la contraseña autoasignada regularmente (cada 30 días y con más frecuencia si se tienen privilegios) evitando reutilizar contraseñas antiguas.

- Mantener la confidencialidad de la contraseña (por ejemplo no escribirla en un papel si no exista forma segura de guardarlo); cambiar la contraseña si se tiene algún indicio o posibilidad de que su confidencialidad pueda verse comprometida.

- No incluir la contraseña en ningún procedimiento automático de conexión o que requiera un cambio de identificador de usuario (por ejemplo en 'scripts' o 'guiones', macros, teclas de función, etc.)

✓ **Equipamiento desatendido asignado al usuario**

Cuando el personal deja de utilizar algún equipo, debe seguir las siguientes normas de seguridad:

- Cancelar todas las sesiones activas antes de marcharse, salvo si se dispone de una herramienta de bloqueo general.
- Desconectarse (log-off) de todas las sesiones con los servidores antes de apagar el equipo.

8.3. Prevención Relativa a los Equipos Críticos

8.3.1. Mantenimiento Preventivo de lo Equipos Críticos

Como parte del plan de prevención se debe considerar, que los servidores cuenten con un mantenimiento preventivo por lo menos dos (2) veces al año.

Para tal fin, PERUPETRO S.A. deberá contar con la garantía de los equipos o con contratos de servicio técnico del proveedor de los mismos.

8.3.2. Relación de Equipos Críticos

A continuación se detallan los equipos de computo con los que cuenta PERUPETRO S.A.

Descripción	Uso	Discos	Periféricos y Accesorios Adicionales	Sistema Operativo	Criticidad asignada por PERUPETRO S.A.
AST Manhattan, Pentium 133, 160Mb RAM.	PDC y Servidor de Archivos	2 SCSI de 9.1 Gb. 1 SCSI de 2 Gb.	Tarjeta de red 3COM, Lectora de CD, Tape de 4mm	Windows NT 4.01	Necesario
Compaq Proliant 1600, 2 procesadores Pentium III de 500 Mhz. 1024 Mb. RAM	Servidor de Base de Datos	3 SCSI de 9.1 GB en Raid 5 y 3 SCSI de 18.2 Gb en Raid 5	Tarjeta de red 3COM, Lectora de CD	Windows NT 4.01	Indispensable
Compaq Proliant 1600, 2 procesadores Pentium III de 500 Mhz. 448 Mb. RAM	Servidor de Correo Electrónico	3 SCSI de 9.1 GB en Raid 5.	Tarjeta de red 3COM, Lectora de CD	Windows NT 4.01	Necesario
Compaq Proliant ML370, 2 procesadores Pentium III de 733 Mhz. 1024 Mb. RAM	Servidor de Aplicaciones ORACLE	3 SCSI de 9.1 GB en Raid 5.	Tarjeta de red 3COM, Lectora de CD	Windows NT 4.01	Indispensable
Compaq Proliant 800, procesador Pentium III de 500 Mhz., 128 Mb. RAM	Firewall	1 SCSI de 4.1 GB.	Tarjeta de red 3COM, Lectora de CD	Windows NT 4.01	Necesario
Compatible, procesador Pentium II de 266 Mhz., 64 Mb. RAM	Equipo para Backup y Consola de Norton Antivirus	1 IDE de 6.4 GB.	Tarjeta de red 3COM, Lectora de CD	Windows NT 4.01	Puede Parar
Compatible, procesador Pentium II de 300 Mhz., 64 Mb. RAM	Equipo para Norton Antivirus para Firewall	1 IDE de 6.4 GB.	Tarjeta de red 3COM, Lectora de CD	Windows NT 4.01	Puede Parar
Dell PowerEdge 240, 667 Mhz, 18 SD RAM	Servidor Parsep de Archivos y Correo Electrónico (Exchange)	1 SCSI de 18.2 GB.	Tarjeta de red, Lectora de CD, Magnetic Tape 4mm	Windows NT 4.01	Necesario

Cuadro Nro. 2 Lista de Equipos de Cómputo de PERUPETRO S.A.

8.4. Prevención Relativa a las Comunicaciones

8.4.1. Mantenimiento Preventivo de los Equipos de Comunicaciones

Como parte del plan de prevención se recomienda que los equipos de comunicaciones cuenten con un mantenimiento periódico de por lo menos 2 veces al año por parte del proveedor de los servicios de comunicaciones.

8.4.2. Relación de Equipos de Comunicaciones

Los Equipos de comunicaciones de PERUPETRO son

Cantidad de Equipos	Descripcion
7	Concentrador 3COM Super Stack II de 12 puertos, Fast Ethernet.
3	Concentrador 3COM Super Stack II dual de 12 puertos, 10/100.
1	Concentrador Dlink de 4 puertos, 10/100.
1	Concentrador 3COM OfficeConect Dual Speed Hub de 8 puertos, 10/100.
1	Concentrador 3COM SuperStack II de 12 puertos.
1	Concentrador 3COM de 8 puertos.
2	Switch 3COM SuperStack 3300 de 24 puertos 10/100, 2 puertos de fibra optica 100mbps
1	Router Cisco 1605 Router.
1	Router Cisco 2600 Router.
2	Ethernet Media Convertor.
1	Auto Switch CYBEX AutoView Commander Dispositivo para conectar ocho computadoras a un monitor, teclado y mouse.

Cuadro Nro. 3 Equipos de Comunicaciones de PERUPETRO S.A.

8.4.3. Internet y Correo Electrónico

Según el estudio realizado para la elaboración del presente Plan de Contingencia los servicios más

importantes para las áreas usuarias son, Correo electrónico y acceso a Internet por lo que se recomienda contar con un enlace alterno de emergencia con un proveedor distinto como por ejemplo servicio satelital de conexión con Internet. Dicha conexión adicional se administrará desde el Firewall de PERUPETRO S.A.

8.4.4. Diagrama de la Red de datos

El siguiente es el Diagrama de red de PERUPETRO S.A.

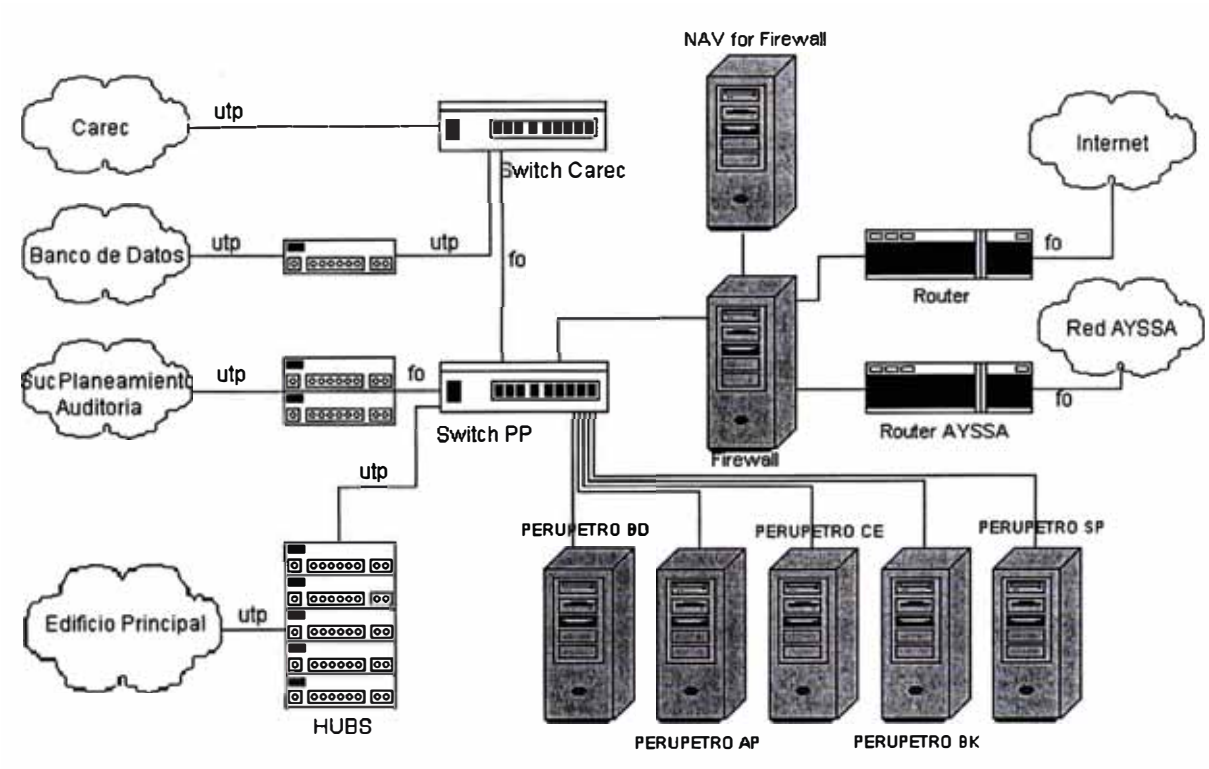


Gráfico Nro. 5 Red de Datos de PERUPETRO S.A.

8.5. Prevención Relativa al Personal

La seguridad referida al personal deberá contemplar desde las etapas de selección del mismo, e incluirá en los contratos y definiciones de puestos de trabajo para poder cumplir el objetivo de reducir los riesgos derivados de actuaciones humanas (errores, robos, fraudes, mal uso de las aplicaciones, etc.)

Se deberá comprobar que las definiciones de puestos de trabajo contemplan todo lo necesario en cuanto a responsabilidades de seguridad de la información y sus sistemas. Las personas que se incorporen a PERUPETRO S.A. deben entrenarse adecuadamente, sobre todo las que lo hagan en áreas de trabajo con información crítica.

8.5.1. Autorizaciones de acceso al ambiente de trabajo

PERUPETRO S.A. deberá entregar pases o fotochecks respectivos al personal de la empresa o al personal de contratistas, para permitir su acceso a las instalaciones, los mismos que serán devueltos cuando dejen de laborar.

Para la entrega de los pases o fotochecks, al inicio y durante la relación laboral del personal de PERUPETRO S.A. o empresas externas se deberá hacer las verificaciones respectivas. Estas verificaciones deberán incluir al menos:

- Examinar cuidadosamente el Currículum Vitae del candidato.
- Contrastar los datos personales y de identificación: D.N.I., L.E., Pasaporte.
- Verificar la información sobre su trabajo en organizaciones anteriores.
- Verificar sus antecedentes policiales.
- Acreditar las certificaciones académicas.
- Analizar las garantías para el puesto a desempeñar especialmente para funciones sensibles de la empresa.

Estas actividades serán efectuadas por el área de recursos humanos o tercerizadas a otras empresas.

Asimismo, para el personal que desarrollará funciones a tiempo parcial o temporal (asesoría, mantenimiento o reparación de equipos y otros) se otorgarán credenciales de visitantes temporales, la información de este personal se deberá verificar bajo el mismo alcance descrito en este punto.

A continuación se adjunta los procedimientos CNTG-PRE-01 y CNTG-PRE-02 relativos a la vigilancia y control de acceso físico de clientes y del personal respectivamente.

PP-PCRD	CNTG-PRE-01 Procedimiento de Vigilancia y Control de Acceso Físico de Clientes	PLNCNTG

Vigilancia y Control de Acceso Físico de Clientes

1. Objetivo

Determinar las normas de seguridad para el control eficiente de ingreso y salida de publico, proveedores y visitantes a las Oficinas de PERUPETRO S.A., para minimizar el riesgo de atentados contra la seguridad del personal y las instalaciones de PERUPETRO S.A.

2. Alcance

El siguiente procedimiento deberá ser de cumplimiento de todo el personal de PERUPETRO S.A., apoyados por el personal de vigilancia.

3. Procedimiento

3.1 Acceso a Oficinas de PERUPETRO S.A.

- Los visitantes o clientes tendrán acceso a las oficinas de PERUPETRO S.A.
- No se permitirá el acceso de vendedores ambulantes y personas con síntomas de ebriedad y/o drogados.
- No se permitirá el ingreso de personas que porten armas de fuego o de otro tipo. Los vigilantes a cargo de PERUPETRO S.A. serán los encargados de hacer cumplir esta disposición
- No se permitirá que los visitantes ingresen a áreas o pisos, para los que no hayan sido autorizadas expresamente.

3.2 Acceso a Oficinas Administrativas

- Los visitantes o clientes que requieran ingresar a las oficinas administrativas deberán identificarse en vigilancia y obtener un pase para la oficina o dependencia a la que deba ingresar canjeándolo por su documento de identidad .
- Se deberá anunciar al visitante y solo permitirle el acceso si el personal de PERUPETRO S.A. lo autoriza.
- Si el visitante no cuenta con documento de identidad se deberá preguntar a la persona de PERUPETRO S.A. con la que desea comunicarse y se le permitirá el acceso bajo la responsabilidad de la persona que autorice el ingreso del visitante.

3.3 Acceso a las Instalaciones de Sistemas

- Se seguirán los pasos señalados en los puntos 3.1 y 3.2 .
- Por tratarse de un área restringida, solo se permitirá el ingreso al Centro de Computo a un visitante si es autorizado por el encargado de sistemas y en todo momento se encontrará acompañado por personal de sistemas autorizado para tal fin.

PP-PCRD	CNTG-PRE-01 Procedimiento de Vigilancia y Control de Acceso Físico del Personal	PLNCNTG

Vigilancia y Control de Acceso Físico del Personal

1. Objetivo

Determinar las normas de seguridad para el control eficiente de ingreso y salida del personal de PERUPETRO S.A.

2. Alcance

El siguiente procedimiento deberá ser de cumplimiento de todo el personal de PERUPETRO S.A., apoyados por el personal de vigilancia.

3. Procedimiento

3.1 Ingreso del Personal

- El área de Recursos Humanos de PERUPETRO S.A. informará la relación detallada de todo el personal, indicando el número de D.N.I., además de los datos personales, antecedentes policiales y labor que realiza.
- Es obligación de PERUPETRO S.A. mantener la relación detallada del personal involucrado en el servicio actualizada.
- PERUPETRO S.A. entregará los pases respectivos para su personal, los mismos que serán devueltos cuando dejen de laborar. RR.HH. informará por escrito a vigilancia, a más tardar dentro de las 24 horas de producido el hecho, adjuntando los pases respectivos.
- Los encargados de seguridad deberán verificar la identidad del personal que ingrese a las instalaciones de PERUPETRO S.A., solo se permitirá el ingreso del personal que porte el pase de ingreso.
- El ingreso o salida de activos (materiales, equipos de cómputo, muebles y enseres) deben estar autorizados por los responsables de PERUPETRO S.A.
- El personal externo de servicio técnico así como cualquier otro proveedor tiene la obligación de presentar una lista del personal que brindará servicios en PERUPETRO S.A. y de actualizarla periódicamente.

Nota: El personal externo deberá sujetarse a las normas de seguridad de acceso de PERUPETRO S.A.

8.5.2. Cláusulas de confidencialidad

El personal de PERUPETRO S.A. firmará cláusulas de seguridad (al menos de confidencialidad) como parte de sus condiciones iniciales de trabajo.

8.5.3. Seguridad de la información en el trabajo

La definición de los puestos de trabajo contemplará las funciones y la responsabilidad de seguridad de sus ocupantes sobre la información y sus sistemas. De ser necesario se incluirá responsabilidades generales para la implementación o mantenimiento de la Política de Seguridad desde el puesto de trabajo, así como responsabilidades específicas para la protección de activos o para la ejecución de procesos o actividades particulares de seguridad. [2]

8.5.4. Adiestramiento del personal

Para garantizar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de los sistemas de información y que están preparados para aplicar la política de seguridad en el curso normal de su trabajo, recibirán formación sobre seguridad y uso correcto de los sistemas de información y de sus facilidades. Al final de dicha formación, los usuarios deberán recibir autorizaciones precisas y se comprometerán, por escrito, a conocer y respetar el

[2] Las políticas de seguridad deben establecerse en base a la normatividad vigente aplicable a PERUPETRO S.A., como por ejemplo las normas técnicas de control establecidas por la Contaduría General de la República.

alcance de sus derechos y las restricciones de acceso a dichos sistemas.

Todo el personal de PERUPETRO S.A. recibirá una formación apropiada en las políticas y procedimientos de la organización que incluya los requerimientos de seguridad y otros controles en su funcionamiento, así como una formación adecuada en el uso correcto de las Tecnologías de Información (procedimientos de 'log-on', uso de aplicaciones y de herramientas software, etc.).

Estas medidas se exigirán antes de obtener el acceso a los servicios y datos, para asegurar que los procedimientos de seguridad se siguen correctamente y se minimizan posibles riesgos para la disponibilidad o integridad de datos o servicios debidos a errores del usuario.

8.5.5. Comportamiento ante incidentes

En caso de ocurrir algún incidente de seguridad o mal funcionamiento de los sistemas, el personal informará lo más rápidamente posible a su jefe inmediato para que se pongan en funcionamiento los mecanismos establecidos para solucionar el incidente. Además, se registrarán dichos incidentes para aprender de estas experiencias, con el objeto de minimizar los daños y otras consecuencias que aquellos pueden provocar en caso ocurrir nuevamente.

Todo el personal de PERUPETRO S.A. deberá conocer los procedimientos que se establezcan para realizar y remitir informes sobre los diferentes tipos de incidentes e infracciones en materia de seguridad, las amenazas, vulnerabilidades o simplemente el mal funcionamiento que puedan tener impacto en la seguridad de los activos de PERUPETRO S.A.

En caso que el usuario sospeche que el mal funcionamiento es debido a problemas de software (por ejemplo un virus), el usuario debe:

- Observar los síntomas y mensajes que aparezcan en pantalla.
- Dejar de usar el sistema (aislarlo si es posible, pero no apagarlo) e informar de inmediato a la unidad de soporte informático.
- Informar inmediatamente a su mando responsable por el canal determinado para la revisión y solución del problema por el personal calificado.

8.5.6. Procedimiento disciplinario

Se establecerá y formalizará un procedimiento disciplinario, sobre la forma de resolver las infracciones en materia de seguridad la cual puede llegar a la separación definitiva del personal en caso sea necesario.

Este procedimiento se aplicará a los empleados que supuestamente hayan violado las políticas y los

procedimientos de seguridad de la Organización. La existencia del procedimiento puede disuadir a los empleados que puedan desatender los requerimientos de seguridad establecidos, y también permitir el tratamiento de empleados sospechosos de cometer violaciones serias y continuadas de procedimientos de seguridad. [3]

[3] Nota: Los procedimientos disciplinarios deben aplicarse teniendo en cuenta la legislación vigente, tanto en materia laboral como en el caso de los delitos informáticos (que establece incluso penas de cárcel para aquellas personas que cometan dichos delitos): así como también las normas y directivas internas de la empresa.

9. PLAN DE EJECUCION

El Plan de Ejecución tiene por finalidad establecer los procedimientos que permitan responder a las contingencias que afecten el normal funcionamiento de los sistemas de PERUPETRO S.A.

Los elementos que conforman el Plan de Ejecución son los relativos a:

- Escenarios de Contingencias y Prioridades de Reposición
- Descripción del Centro de Procesamiento de Respaldo - CPR
- Procedimientos de Contingencias según las Fuentes de Origen
- Cartillas de respuestas a Contingencias, por cada equipos responsables de enfrentar el problema

9.1. Escenarios de Contingencias y Prioridades de Reposición

9.1.1. Escenarios de Contingencias

El Plan de Contingencia considera la provisión de la Plataforma Informática necesaria que le permita continuar sus operaciones ante un evento extraordinario e imprevisible que inutilice parcial o completamente el funcionamiento de sus servidores centrales ubicados en la oficina principal de PERUPETRO S.A.; ello incluye incendios, inundaciones, derrumbes, terremotos, huelgas o tomas de local que impidan la entrada al mismo, atentados terroristas y otros actos vandálicos y eventos similares.

Para el establecimiento de los escenarios se considerarán tres áreas desastres posibles :

- Desastre en el Centro de Cómputo (Oficina Principal).
- Desastre en Áreas Usuarias.
- Desastre en la Oficina del Banco de Datos.

Se consideran los siguientes Escenarios de Contingencias severas o desastres:

	Centro de Cómputo	Áreas Usuarias	Banco de Datos	Respuesta
Escenario 1:	Inhabilitado	Operativa	Operativo	CPR
Escenario 2:	Operativo	Inhabilitado	Operativo	Ambiente alternativo de emergencia
Escenario 3:	Inhabilitado	Inhabilitado	Operativo	CPR + Ambiente alternativo de emergencia
Escenario 4:	Operativo	Operativo	Inhabilitado	Oficina Principal de Schlumberger

Cuadro Nro. 4 Escenarios de Contingencia – Resumen

Escenario	Respuesta	Observación
Escenario 1 • Inhabilitación severa del Centro de Cómputo de la Oficina Principal de PERUPETRO S.A. • Áreas usuarias, Operativas. • Banco De Datos operativo	• Traslado de operaciones al Centro de Procesamiento de Respaldo CPR. • Operaciones continúan de manera restringida con información del CPR.	No se contará con un enlace de contingencia entre el CPR y las oficinas de PERUPETRO S.A.
Escenario 2 • Centro de Cómputo de PERUPETRO S.A. Operativo. • Inhabilitación de alguna de las áreas Usuarias • Banco de Datos operativo	• Traslado a un Ambiente alternativo de emergencia. • Operaciones continúan en Centro de Cómputo de PERUPETRO S.A.	No se contará con enlace de contingencia entre el Centro de Cómputo de PERUPETRO S.A. y el ambiente alternativo de emergencia.
Escenario 3 • Inhabilitación severa del Centro de Cómputo de PERUPETRO S.A. • Inhabilitación áreas usuarias • Banco de Datos operativo	• Traslado de operaciones al Centro de Procesamiento de Respaldo CPR. • Traslado al Ambiente alternativo de Emergencia	No se contará con enlace de contingencia entre el CPR y el ambiente alternativo de emergencia.
Escenario 4 • Centro de Cómputo de PERUPETRO S.A. operativo • Áreas usuarias operativas • Inhabilitación de la Oficina del Banco de Datos.	• Traslado de operaciones y habilitación de local Principal de Schlumberger para el servicio de Banco de Datos.	Se rehabilitará la Operación del Banco de Datos en forma normal luego de haber rehabilitado el local principal de PERUPETRO S.A.

Cuadro Nro. 5 Escenarios de Contingencia - Detallado

✓ Desastre en el Centro de Cómputo de PERUPETRO S.A.

En el caso que ocurra un desastre en el Centro de Cómputo implementado en el local principal de PERUPETRO S.A., que impida su normal funcionamiento, se ha considerado la contratación de un Centro de Procesamiento de

Respaldo (CPR) el cual contará con el ambiente, equipos de respaldo, mobiliario y con la infraestructura de cableado eléctrico y de datos probado y operativo, que cumplan las especificaciones técnicas para el óptimo funcionamiento de los equipos de respaldo.

- ✓ **Desastre en Áreas Usuarias**

  En el caso que ocurra un desastre en las áreas usuarias, PERUPETRO S.A. se encargará de la habilitación de la Oficina alternativa de emergencia en los ambientes que se asignen para este servicio.

  PERUPETRO S.A. deberá habilitar esta oficina alternativa de emergencia con los equipos, mobiliario, cableado eléctrico y cableado de datos que sean necesarios para reponer el servicio afectado, de acuerdo a la criticidad del mismo.

- ✓ **Desastre en la Oficina del Banco de Datos**

  En el caso que ocurra un desastre en las Oficinas asignadas al servicio de Banco de Datos en el local principal de PERUPETRO. S.A., el contratista de la administración del Banco de Datos (actualmente la Compañía SCHLUMBERGER), se encargará de la habilitación de un centro alternativo de respaldo y rehabilitará las operaciones según lo estipulado en el contrato de servicios.

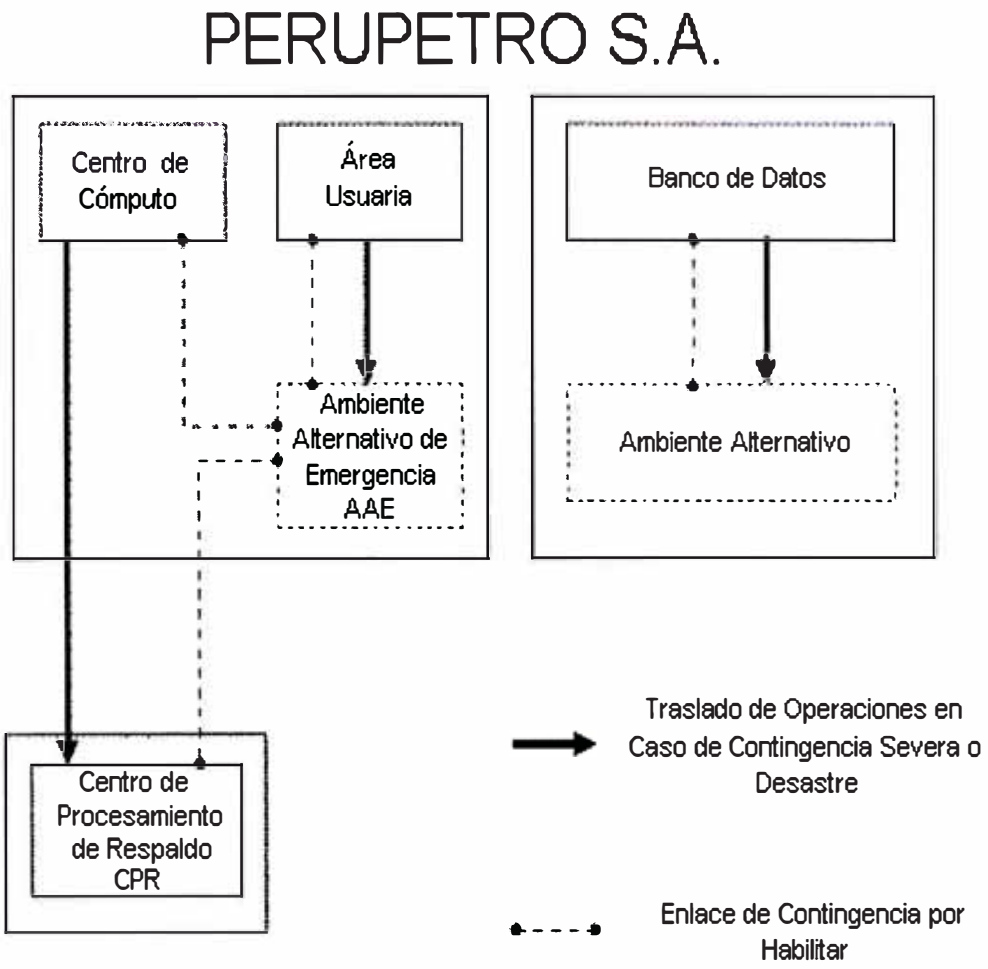


Gráfico Nro. 6 Flujo de Respuesta a Contingencias

9.1.2. Prioridades de Reposición

Los recursos disponibles serán usados para recuperar y reponer funciones basadas en su criticidad e importancia para la continuidad de la operación de la organización. A continuación identificamos los sistemas a ser repuestos en orden de prioridad de acuerdo al

tiempo que pueda tomar la rehabilitación de los servicios involucrados. [4]

Nro.	Sistema	Prioridad
1.	Sistema de Comercialización SICOVHI.	Alta
2.	Acceso a Internet.	Alta
3.	Correo Electrónico.	Alta
2.	Sistema de Gestión Administrativa Financiera SIGAF.	Media
3.	Sistema de Trámite Documentario.	Baja
4.	Sistema de Control de Tareas.	Baja

Cuadro Nro. 6 Prioridades de Reposición

Las reuniones realizadas con cada una de las gerencias y las encuestas usadas en estas reuniones permiten determinar una estimación de los tiempos de rehabilitación, tal como se muestra en el Cuadro Nro. 7.

Ítem	Prioridad	Tiempo Máximo De Parada	Tiempo Máximo De Rehabilitación
1.	Alta	12 horas	24 horas
2.	Media	24 horas	48 horas
3.	Baja	48 horas	72 horas

Cuadro Nro. 7 Estimación de Tiempo Máximo de Rehabilitación

Donde:

- **Tiempo de Parada:** es el tiempo máximo que se puede tolerar antes de implementar el plan de contingencia.

[4] **Nota Importante:** No se incluyen dentro de esta relación los sistemas de terceros que corren en estaciones de trabajo tales como el sistema de pago a proveedores - Pay Link de Citibank, el Sistema de Declaración Telemática – PDT de Sunat, y Sistema de Información Legal de Infolex

- **Tiempo de Rehabilitación:** es el tiempo máximo que puede transcurrir desde el inicio del plan hasta el reinicio de las operaciones.

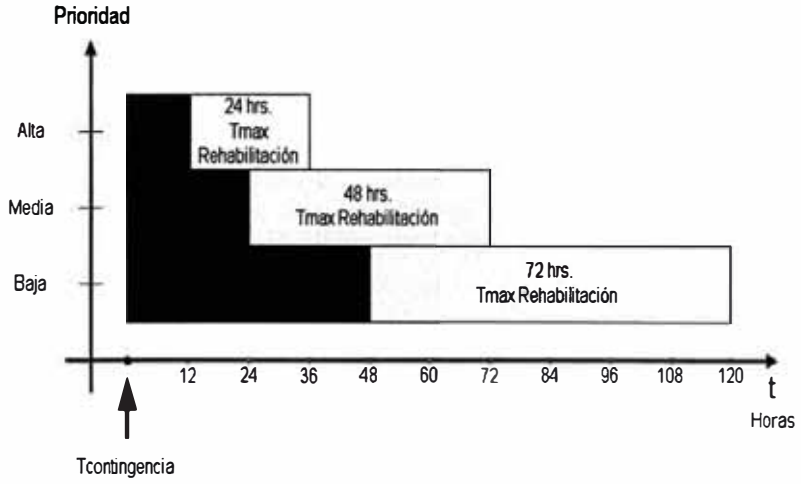


Gráfico Nro. 7 Tiempos Máximos de Parada y Rehabilitación

9.2. Descripción del Centro de Procesamiento de Respaldo – CPR

9.2.1. Ubicación y Características del CPR

El Centro de Procesamiento de respaldo estará disponible en las oficinas del proveedor del servicio los 365 días del año, es recomendable que el CPR no se encuentre a menos de 1 km. ni a más de 10 km. de la oficina principal de PERUPETRO S.A. para minimizar riesgos y optimizar los tiempos de traslado de operaciones e información.

Este Centro de Procesamiento deberá contar con las siguientes características:

Ítem	Aspecto	Características
1	Espacio Físico	El CPR dispondrá del espacio suficiente para proveer la continuidad del servicio en caso de una contingencia.
2	Seguridad	El CPR contará con servicios de vigilancia y control de acceso del personal. Así mismo con un Sistema de detección de humo, calor, sensor de aniego, extintor contra incendio y chapa eléctrica de seguridad en la puerta.
3	Mobiliario	El proveedor del servicio dispondrá del mobiliario suficiente para albergar y garantizar la continuidad de la operaciones de PERUPETRO S.A. en un caso de contingencia.
4	Comunicaciones	El CPR contará con central telefónica y disponibilidad de anexos para cubrir los requerimientos de los usuarios de PERUPETRO S.A.
5	Red	El CPR contará con cableado estructurado y puntos de conexión suficientes para comunicar los equipos de respaldo con los usuarios instalados en el CPR
6	Mantenimiento de local	El CPR contará con servicios básicos de alimentación eléctrica, agua y limpieza necesarios para albergar a los usuarios de PERUPETRO S.A.
7	Centro de Cómputo	El CPR contará con un Centro de Cómputo especialmente acondicionado para dicho fin, donde estarán ubicados los equipos de respaldo.
8	Acceso a Internet	El CPR contará con los accesos necesarios a Internet para los usuarios de PERUPETRO S.A. que trasladen sus operaciones al CPR.
9	Correo Electrónico	El Proveedor del Servicio asignará cuentas genéricas de correo electrónico para los usuarios de PERUPETRO S.A. que trasladen sus operaciones al CPR.
10	Almacenamiento de Copias de Respaldo (Backups)	El CPR contará con un área especifica para el almacenamiento de las copias de respaldo con las características y condiciones requeridas para tal fin.

Cuadro Nro. 8 Características del Centro de Procesamiento de Respaldo

Adicionalmente, el CPR deberá contar con los equipos y programas que servirán de respaldo para dar continuidad a las operaciones de PERUPETRO S.A., en los casos de inhabilitación mayor del local principal, o de los equipos críticos.

9.2.2. Infraestructura de Respaldo en el CPR

El Centro de Procesamiento de respaldo deberá contar con los siguientes elementos :

- UPS de 6 KVA para los equipos de respaldo, con un tiempo de autonomía de 30 minutos.
- Grupo Electrógeno.

9.2.3. Equipos de Respaldo en el CPR

En el Centro de Procesamiento de Respaldo, la plataforma de respaldo considerada deberá ser la siguiente:

- 2 Servidor Compaq Proliant 1600 con 2 procesadores Pentium III Xeon de 500 Mhz, 1024 MB RAM y arreglo de 3 discos de 18.2 GB, con componentes internos redundantes como son fuente de poder y Controladora Smart Array 5304 con 128 MB de memoria Caché de cuatro canales Ultra3 para el arreglo de Discos.
- 1 Switch Catalyst 3524 (Opcional).
- 1 Router Cisco 2650 (Opcional).
- 1 Impresora láser.

- 5 estaciones de trabajo conectadas en red para usuarios de las aplicaciones.
- Con respecto al software base incluido en esta plataforma, se considera, Microsoft Windows NT Server 4.0, Microsoft SQL Server 7.0, Oracle 8.x, Oracle Financial, Microsoft Exchange Server 5.6.

9.3. Procedimientos de Contingencias según las Fuentes de Origen

Las fuentes de contingencias cubiertas por este plan y las acciones a ejecutar para cada una de ellas se detallan a continuación. Estas fuentes de contingencias se refieren usualmente a diferentes grados dentro de 6 categorías principales: local principal, equipos críticos, comunicaciones de voz y datos, software base y aplicaciones, personal clave y datos. La causa de la pérdida se determina luego del diagnóstico que se realiza, siendo el primer objetivo del plan de ejecución determinar el grado de pérdida, el impacto en la misión y las técnicas para minimizar este riesgo.

9.3.1. Pérdida de local principal

Generalmente la inhabilitación de las instalaciones o del local se debe a alguna catástrofe o desastre, tales como un incendio, inundación, terremoto, etc. Sin embargo, una pérdida temporal puede deberse a una falla en la alimentación de energía eléctrica, falla del aire acondicionado, filtración de agua, u otros eventos que pueden redundar en la inhabilitación de las instalaciones y

por tanto en una pérdida mensurable de capacidad operativa.

A continuación se detalla el procedimiento **CNTG-EJC-01** denominado **Procedimiento de Respuesta en Caso de Pérdida de Local Principal**

PP-PCRD	CNTG-EJC-01 Procedimiento de Respuesta en Caso de Pérdida de Local Principal	PLNCNTG
Rev. 1.0		Pág. 1 de 2

Procedimiento de Respuesta en Caso de Pérdida de Local Principal

A continuación se detalla el procedimiento de rehabilitación en caso de desastre o pérdida del local de PERUPETRO S.A.

1. Objetivo

Recuperar la capacidad operativa, en el caso que el local de PERUPETRO S.A. sufra alguna contingencia que imposibilite el funcionamiento del servicio.

2. Responsabilidades

Es responsabilidad del Coordinador del Plan de Contingencia controlar el cumplimiento del presente procedimiento.

El Equipo de Soporte conformado por personal externo de soporte técnico, es responsable de ejecutar los procedimientos necesarios para restaurar el equipo, el software y las aplicaciones en el menor tiempo posible.

3. Procedimiento

3.1 Se reportará al Coordinador del Plan de Contingencia la ocurrencia del incidente.

3.2 El Coordinador del Plan de Contingencia reportará el incidente a la Gerencia General de PERUPETRO S.A. y contactará a todo el personal de soporte involucrado en el esfuerzo de reposición.

3.3 El Coordinador del Plan de Contingencia mediante llamada telefónica al Personal de Seguridad de la empresa encargada del CPR, autorizará el ingreso al local del CPR del personal de PERUPETRO S.A. Copia de la relación de este personal se encontrará en poder del personal de Seguridad de PERUPETRO S.A. y del CPR.

3.4 El equipo de manejo de emergencia con la ayuda del equipo de soporte realizará las siguientes labores:

- Diagnóstico y detección de la inhabilitación del local.
- Determinación del grado de pérdida y el impacto de la misma.
- Se informará al Coordinador del Plan sobre el estado del incidente, y a los usuarios afectados, el tiempo esperado de normalización de operaciones.

3.5 El Coordinador del Plan informará a la Gerencia General de PERUPETRO S.A. el estado de la contingencia y solicitará la autorización para el traslado de las operaciones al Centro de Procesamiento de Respaldo – CPR.

PP-PCRD	CNTG-EJC-01 Procedimiento de Respuesta en Caso de Pérdida de Local Principal	PLNCNTG
Rev. 1.0		Pág. 2 de 2

3.6 Una vez aprobado el traslado de las operaciones al Centro de Procesamiento de Respaldo, el Equipo de Emergencia coordinará con el equipo de soporte el inicio de las acciones de contingencia en el CPR.

3.7 El equipo de soporte iniciará la configuración y arranque de los equipos del centro de procesamiento de respaldo.

3.8 Luego se procederá a restaurar el Software, la Base de Datos y los Datos con la información contenida en las cintas backup ubicadas en el Centro de Procesamiento de Respaldo CPR (la restauración se debe trabajar con los últimos backups realizados).

3.9 Una vez operativo el equipo, se restablecerá el proceso y el servicio, y se siguen las misma políticas de prevención que en la oficina principal.

3.10 Se procede a documentar el incidente indicando el tiempo que tomó restablecer las operaciones.

3.11 Se comunicará a la empresa encargada del CPR el cierre del incidente.

4. Tiempos estimados

4.1 Para el inicio de actividades en el CPR:

- Tiempo promedio: 4 horas
- Tiempo Máximo: 8 horas

9.3.2. Pérdida de equipos críticos

En caso de ocurrir una contingencia que lleve a la pérdida de algún equipo critico, se ha establecido el siguiente procedimiento **CNTG-EJC-02** denominado **Procedimiento de Respuesta en Caso de Pérdida de Equipos Críticos**

PP-PCRD	CNTG-EJC-02 Procedimiento de Respuesta en Caso de Pérdida de Equipos Críticos	PLNCNTG
Rev. 1.0		Pág. 1 de 1

Procedimiento de Respuesta en Caso de Pérdida de Equipos Críticos

En caso de ocurrir una contingencia que lleve a la pérdida de algún equipo, se ha establecido el siguiente procedimiento.

1. Objetivo

La reparación efectiva y confiable del equipo para devolver el mismo a su estado de operación normal en el menor tiempo posible.

2. Responsabilidades

Es responsabilidad del Coordinador del Plan de Contingencia controlar el cumplimiento del presente procedimiento.

El equipo de soporte conformado por el personal externo de soporte técnico, es responsable de efectuar la reparación y puesta en operatividad de los equipos.

3. Procedimiento

3.1 Se reportará al Coordinador del Plan de Contingencia la ocurrencia del incidente.

3.2 El coordinador del Plan de Contingencia reportará el incidente al equipo de manejo de emergencias el cual se encargara de contactar a todo el personal de soporte involucrado en el esfuerzo de reposición.

3.3 El equipo de soporte realizará las siguientes labores:

- Diagnóstico y detección de la falla en el equipo.
- Determinación del grado de pérdida, el impacto de la misma y las acciones a tomar dependiendo del grado de contingencia (reparación del equipo o traslado al centro de procesamiento de respaldo).
- Se informará al Coordinador del Plan sobre el estado del incidente, y a los usuarios afectados el tiempo esperado de normalización de operaciones.

3.4 Si se opta por la reparación del equipo, el técnico de soporte asignado solicita el repuesto de la parte dañada al proveedor, para proceder a realizar el reemplazo, y envía la parte dañada a servicio técnico del proveedor para su reparación.

3.5 Se procederá con el cambio de la parte dañada.

3.6 Se realizarán los diagnósticos y pruebas de funcionamiento.

3.7 En caso de seguir presentando algún problema, se vuelven a repetir los pasos desde el ítem 3.3.

3.8 De pasar bien las pruebas, se informa al coordinador del plan de contingencia a fin de proceder a entregar el equipo y ponerlo operativo y se comunica a los usuarios afectados el restablecimiento del servicio.

3.9 Se procede a documentar el incidente indicando el tiempo de reparación del equipo y el tiempo de prueba en que el equipo ha sido probado.

4. Tiempos estimados

4.2 Para el inicio de actividades en el CPR:

- Tiempo promedio: 4 horas
- Tiempo Máximo: 8 horas

9.3.3. Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones.

Para los casos de pérdida de comunicaciones se han establecido los procedimientos **CNTG-EJC-03 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones Datos y CNTG-EJC-04 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones – Voz.**

PP-PCRD	CNTG-EJC-03 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones – Datos	PLNCNTG
Rev. 1.0		Pág. 1 de 1

Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones – Datos

1. Objetivo

El restablecimiento de las comunicaciones de datos a su estado de operación normal en el menor tiempo posible.

2. Responsabilidades

Es responsabilidad del Coordinador del Plan de Contingencia controlar el cumplimiento del presente procedimiento.

El equipo de soporte es responsable de efectuar la reparación y puesta en operatividad de los equipos.

3. Procedimiento

3.1 Se reportará al Coordinador del Plan de Contingencia la ocurrencia del incidente.

3.2 El Coordinador del Plan de Contingencia reportará el incidente y contactara a todo el personal de soporte involucrado en el esfuerzo de reposición.

3.3 El Coordinador del plan con la ayuda del equipo de soporte, realizarán las siguientes labores:

- Diagnóstico y detección de la falla en el equipo.
- Determinación del grado de pérdida, el impacto de la misma y las acciones a tomar dependiendo del grado de contingencia (reparación del equipo o traslado al centro de procesamiento de respaldo).
- Se informará al Coordinador del Plan sobre el estado del incidente, y a los usuarios afectados, el tiempo esperado de normalización de operaciones.

3.4 Si se opta por la reparación del equipo, el técnico de soporte asignado solicita el repuesto de la parte dañada al proveedor para proceder a realizar el reemplazo y envía la parte dañada a servicio técnico del proveedor para su reparación.

3.5 Se procede con el cambio de la parte dañada.

3.6 Se realizan los diagnósticos y pruebas de funcionamiento.

3.7 En caso de seguir presentando algún problema, se vuelven a repetir los pasos desde el ítem 3.3.

3.8 De pasar bien, se informará al Coordinador del Plan de Contingencia a fin de proceder a entregar el equipo y ponerlo operativo y se comunicará a los usuarios afectados el restablecimiento del servicio.

3.9 Se procederá a documentar el incidente indicando el tiempo de reparación del equipo y el tiempo de prueba en que el equipo ha sido probado.

4. Tiempos estimados

Para el inicio de actividades en el CPR:

- Tiempo promedio: 2 horas
- Tiempo Máximo: 6 horas

PP-PCRD	CNTG-EJC-04 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones – Voz	PLNCNTG
Rev. 1.0		Pág. 1 de 1

Procedimiento de Respuesta en Caso de Pérdida de comunicación - Voz

1. Objetivo

El restablecimiento de las comunicaciones de Voz en el menor tiempo posible.

2. Responsabilidades

Es responsabilidad del Coordinador del Plan de Contingencia controlar el cumplimiento del presente procedimiento.

3. Procedimiento

3.1 Se reportará al Coordinador del Plan de Contingencia la ocurrencia del incidente.

3.2 El coordinador del Plan de Contingencia reportará el incidente a todo el personal involucrado en el servicio y a la Gerencia General de PERUPETRO S.A. indicándole los números de celular por los que se pueden realizar las comunicaciones mientras se restablece el servicio de voz.

3.3 Mientras dure la contingencia, el personal de PERUPETRO S.A. deberá tener disponibles teléfonos celulares o radios para la gerencia y jefaturas, para las coordinaciones operativas.

4. Tiempos estimados

Para el inicio de actividades en el CPR:

- Tiempo promedio: 1 horas
- Tiempo Máximo: 4 horas

9.3.4. Procedimiento de Respuesta en Caso de Perdida de Software Base y Aplicaciones

En caso de ocurrir una contingencia que lleve a la Perdida de Software Base y Aplicaciones, se ha establecido el siguiente procedimiento **CNTG-EJC-05 Procedimiento de Respuesta en Caso de Pérdida de Software Base y Aplicaciones.**

PP-PCRD	CNTG-EJC-05 Procedimiento de Respuesta en Caso de Pérdida de Software y Aplicaciones	PLNCNTG
Rev. 1.0		Pág. 1 de 129

Procedimiento de Respuesta en Caso de Pérdida de Software y Aplicaciones

1. Objetivo

El restablecimiento del Software y aplicaciones relevantes en el menor tiempo posible, ante un evento en el cual el software base y/o las aplicaciones se dañen o corrompan.

2. Responsabilidades

Es responsabilidad del Coordinador del Plan de Contingencia controlar el cumplimiento del presente procedimiento.

El personal de soporte técnico se encargará de ejecutar los procedimientos necesarios para restaurar, reinstalar o reconfigurar el software dañado o perdido.

3. Procedimiento

3.1 Se reportará al Coordinador del Plan de Contingencia la ocurrencia del incidente.

3.2 El coordinador del Plan de Contingencia reportará el incidente y contactará a todo el personal de soporte involucrado en el esfuerzo de reposición.

3.3 El Coordinador del plan con la ayuda del equipo de soporte, realizarán las siguientes labores:

- Diagnóstico y detección de la falla en el equipo.
- Determinación del grado de pérdida, el impacto de la misma y las acciones a tomar dependiendo del grado de contingencia (reparación del equipo o traslado al centro de procesamiento de respaldo).
- Se informará al Jefe de la División de Planeamiento sobre el estado del incidente, y a los usuarios afectados, el tiempo esperado de normalización de operaciones.

3.4 Se realizan los diagnósticos y pruebas de funcionamiento.

3.5 En caso de seguir presentando algún problema, se vuelven a repetir los pasos desde el ítem 3.3.

3.6 De pasar bien, se informará al Coordinador del Plan de Contingencia a fin de proceder a entregar el equipo y ponerlo operativo y se comunicará a los usuarios afectados el restablecimiento del servicio.

3.7 Se procederá a documentar el incidente indicando el tiempo de reparación del equipo y el tiempo de prueba en que el equipo ha sido probado.

4. Tiempos estimados

Para el inicio de actividades en el CPR:

- Tiempo promedio: 6 horas
- Tiempo Máximo: 12 horas

9.3.5. Procedimiento de Respuesta por Pérdida o Ausencia de Personal Clave

En caso de ocurrir una contingencia que lleve a la Perdida o Ausencia de Personal Clave, se ha establecido el siguiente procedimiento **CNTG-EJC-06 Procedimiento de Respuesta en Caso de Pérdida de Personal Clave.**

PP-PCRD	CNTG-EJC-06 Procedimiento de Respuesta en Caso de Pérdida de Personal Clave	PLNCNTG
Rev. 1.0		Pág. 1 de 1

Procedimiento de Respuesta en caso de Perdida de Personal Clave

1. Objetivo

El restablecimiento de las operaciones de la División de Planeamiento en el menor tiempo posible, ante la eventual salida o ausencia del personal clave del área de sistemas.

2. Responsabilidades

Es responsabilidad del equipo de Manejo de emergencias controlar el funcionamiento del presente procedimiento.

3. Procedimiento

3.1 Se reportará al coordinador del Plan de Contingencia la ocurrencia del incidente o en su defecto al Jefe de la División de Planeamiento.

3.2 El coordinador del plan reportará el incidente al equipo de manejo de la emergencia.

3.3 El equipo de manejo de la emergencia determinará y evaluará los tiempos máximos de ausencia y de rehabilitación.

3.4 De pasar el tiempo máximo de ausencia se deberá buscar por medio de Recursos Humanos o una empresa tercerizada el reemplazo para el personal critico ausente.

4. Tiempos estimados

Para el inicio de actividades en el CPR:

- Tiempo promedio: 1 día
- Tiempo Máximo: 2 días

Nivel	Personal	Tiempo estimado máximo de ausencia	Tiempo estimado máximo de rehabilitación
Operativo	• Personal externo.	01 día	01 día
Supervisor	• Coordinador de Sistemas. • Administrador General.	02 días	01 día
Jefaturas	• Jefe de División de Planeamiento.	05 días	02 días
Gerencial	• Gerentes de Área • Gerente General	05 días	02 días

Cuadro Nro. 9 Relación de Personal Crítico

Tiempo máximo de ausencia: Es el tiempo máximo que una persona puede ausentarse de la empresa sin que afecte la productividad del área.

Tiempo máximo de rehabilitación: Es el tiempo máximo en que se debe rehabilitar o remplazar al personal ausente de la empresa.

9.3.6. Procedimiento de Respuesta en Caso de Perdida Datos Relevantes

En caso de ocurrir una contingencia que lleve a la pérdida Datos Relevantes, se ha establecido el siguiente procedimiento **CNTG-EJC-07 Procedimiento de Respuesta en Caso de Pérdida de Datos Relevantes.**

PP-PCRD	CNTG-EJC-07 Procedimiento de Respuesta en Caso de Pérdida de Datos Relevantes	PLNCNTG
Rev. 1.0		Pág. 1 de 1

Procedimiento de Respuesta en Caso de Pérdida de Datos

La recuperación de archivos de datos, puede ser ejecutada con la autoridad del coordinador de Sistemas.

1. Objetivo

Recuperar la información de los Sistemas en el menor tiempo posible, ante un evento por el cual éstos se dañen o corrompan.

2. Responsabilidades

Es responsabilidad del Coordinador del Plan de Contingencia controlar el cumplimiento del presente procedimiento.

El personal de soporte técnico es responsable de ejecutar los procedimientos necesarios para restaurar la información pérdida.

3. Procedimiento

3.1 Se reportará al Coordinador del Plan de Contingencia la ocurrencia del incidente.

3.2 El Coordinador del Plan de Contingencia reportará el incidente y contactará a todo el personal de soporte involucrado en el esfuerzo de reposición.

3.3 El Coordinador del plan con la ayuda del equipo de soporte realizarán las siguientes labores:

- Diagnóstico y detección de la falla en el equipo
- Determinación del grado de pérdida, el impacto de la misma y las acciones a tomar dependiendo del grado de contingencia.
- Se informará al Jefe de la División de Planeamiento sobre el estado del incidente, y a los usuarios afectados, el tiempo esperado de normalización de operaciones.

3.4 El Equipo de Soporte Técnico asignado solicitará el último backup disponible para realizar la restauración de la información. De ser necesario solicitará el cambio de disco si éste está dañado y procede a la restauración de la información.

3.5 El Equipo de Soporte Técnico realizará los diagnósticos y pruebas de funcionamiento.

3.6 En caso de seguir presentando algún problema, se vuelven a repetir los pasos desde el ítem 3.3.

3.7 De pasar bien, se informará al Coordinador del Plan de Contingencia a fin de proceder a restaurar el proceso y se comunica a los usuarios afectados el restablecimiento del servicio.

3.8 Se procederá a documentar el incidente indicando el tiempo en que se solucionó el mismo.

4. Tiempos estimados

Para el inicio de actividades en el CPR:

- Tiempo promedio: 8 horas
- Tiempo Máximo: 12 horas

9.4. Cartilla de Respuesta a Contingencias

9.4.1. Coordinador del Plan de Contingencia

- **Objetivo**
  Establecer una pauta de acción ante casos de contingencia que permita ordenar los esfuerzos de reacción y remediación con prontitud y eficacia.

- **Alcances**
  Dirigido al Coordinador de Sistemas

- **Responsabilidades**

  El Coordinador de Sistemas asumirá dentro de sus funciones, la coordinación del Plan de Contingencia. Sus responsabilidades principales serán:

  - ✓ Actuar como el contacto primario en caso de contingencias y coordinar los esfuerzos de recuperación o reposición de la contingencia.
  - ✓ Contactar todo el personal de soporte involucrado en el esfuerzo de reposición.
  - ✓ Proveer a todo el personal externo de soporte una copia actualizada del plan de contingencia.
  - ✓ Contactar a las siguientes personas, tan pronto como sea posible: Gerente General, Jefe de La División de Planeamiento y al Personal externo de soporte de PERUPETRO S.A. .
  - ✓ Ejecutar el plan de contingencia.
  - ✓ Contactar a los usuarios principales de las aplicaciones y asegurar su participación en el proceso de recuperación.

- **Procedimiento Ante una Contingencia**

El coordinador del Plan de Contingencia recepcionará el aviso de la ocurrencia de una contingencia por parte de los usuarios, el personal de sistemas o el personal externo de soporte.

El Coordinador del pan de contingencia deberá evaluar la posible fuente de la contingencia y aplicar el (o los) procedimiento(s) que sean aplicable(s) de los que se detallan a continuación:

- CNTG-EJC-01 Procedimiento de Respuesta en Caso de Pérdida de Local Principal.
- CNTG-EJC-02 Procedimiento de Respuesta en Caso de Pérdida de Equipos Críticos.
- CNTG-EJC-03 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones de Voz.
- CNTG-EJC-04 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones de Datos.
- CNTG-EJC-05 Procedimiento de Respuesta en Caso de Pérdida de Software Base y Aplicaciones.
- CNTG-EJC-06 Procedimiento de Respuesta en Caso de Pérdida de Personal Clave.

  CNTG-EJC-07 Procedimiento de Respuesta en Caso de Pérdida de Datos.

9.4.2. Equipo de Apoyo

- **Objetivo**

Establecer una pauta de acción ante casos de contingencia que permita ordenar los esfuerzos de reacción y remediación con prontitud y eficacia.

- **Alcances**

Dirigido a :

Coordinador de Sistemas.
Coordinadores que los Gerentes de área designen.
Secretarias.

- **Responsabilidades**

Estará integrado por: Coordinador de Sistemas, Coordinadores que los Gerentes de área designen y secretarias. Sus responsabilidades serán:

- ✓ Notificar a los usuarios de la contingencia y dar un estimado del tiempo necesario para la reposición de las operaciones.
- ✓ Coordinar el transporte para el Centro de Procesamiento de Respaldo.
- ✓ Realizar todas las llamadas telefónicas requeridas
- ✓ Ordenar los suministros y papel necesarios reponer las operaciones.
- ✓ Ayudar a los usuarios en la realización de tareas manuales que permitan avanzar con el trabajo pendiente a pesar de la contingencia.

- **Procedimiento Ante una Contingencia**

El Equipo de Apoyo se encargará de servir como nexo entre el Coordinador del Plan y las áreas usuarias durante la contingencia.

El Equipo de Apoyo deberá brindar apoyo logístico y coordinar el traslado de las operaciones al CPR según los procedimientos que se detallan a continuación:

- ✓ CNTG-EJC-01 Procedimiento de Respuesta en Caso de Pérdida de Local Principal.
- ✓ CNTG-EJC-02 Procedimiento de Respuesta en Caso de Pérdida de Equipos Críticos.
- ✓ CNTG-EJC-03 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones de Voz
- ✓ CNTG-EJC-04 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones de Datos
- ✓ CNTG-EJC-05 Procedimiento de Respuesta en Caso de Pérdida de Software Base y Aplicaciones
- ✓ CNTG-EJC-06 Procedimiento de Respuesta en Caso de Pérdida de Personal Clave.
- ✓ CNTG-EJC-07 Procedimiento de Respuesta en Caso de Pérdida de Datos.

9.4.3. Equipo de Manejo de la Emergencia

- **Objetivo**

  Establecer una pauta de acción ante casos de contingencia que permita ordenar los esfuerzos de reacción y remediación con prontitud y eficacia.

- **Alcances**

  Dirigido a:

Gerente de Administración

Jefe de División de Planeamiento

Coordinador de Sistemas

- **Responsabilidades**
  Este equipo estará integrado por: Gerente de Administración, Jefe de División de Planeamiento y el Coordinador de Sistemas de PERUPETRO S.A. (y/o las personas que ellos decidan asignar). Sus responsabilidades principales serán:
  - ✓ Evaluación de la contingencia o del daño (GA, JP).
  - ✓ Proveer rápidamente de un informe del estado de la contingencia al Coordinador del Plan de Contingencia (JP).
  - ✓ Contactar a los recursos externos y/o proveedores necesarios para restaurar los servicios afectados por la contingencia (JP,CS).
  - ✓ Proveer de información relativa a la contingencia al personal afectado (GA, JP, CS).
  - ✓ Determinar las prioridades. Debe haber un período mínimo aceptable en que las operaciones se desarrollarán degradadas, antes de que el plan de recuperación y reposición se implemente.
  - ✓ Asegurar que sea contactado todo el personal externo de soporte que se requiera (ST), a fin de proveer asistencia oportuna(JP, CS).
  - ✓ Determinar el tiempo que tomará restaurar las operaciones completamente (JP,CS).[5]

- **Procedimiento Ante una Contingencia**
  El Equipo de Manejo de la Emergencia se encargará de evaluar la contingencia y comunicar la ocurrencia

[5] Para el párrafo anterior y de aquí en adelante usaremos la siguiente nomenclatura:
- ➢ Gerente de Administración (GA)
- ➢ Jefe de División de Planeamiento (JP)
- ➢ Coordinador de Sistemas (CS)
- ➢ Personal Externo de Soporte Técnico (ST)

de la misma al Coordinador del Plan de Contingencia.

El Equipo de Manejo de la emergencia designará al personal que crea necesario para la recuperación de las operaciones de PERUPETRO S.A. especialmente en el caso de perdida de local principal.

El Equipo de Manejo de la Emergencia deberá coordinar directamente con el Coordinador del Pan de Contingencia en la ejecución y aplicación de los procedimientos que se detallan a continuación:

- ✓ CNTG-EJC-01 Procedimiento de Respuesta en Caso de Pérdida de Local Principal.
- ✓ CNTG-EJC-02 Procedimiento de Respuesta en Caso de Pérdida de Equipos Críticos.
- ✓ CNTG-EJC-03 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones de Voz.
- ✓ CNTG-EJC-04 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones de Datos.
- ✓ CNTG-EJC-05 Procedimiento de Respuesta en Caso de Pérdida de Software Base y Aplicaciones.
- ✓ CNTG-EJC-06 Procedimiento de Respuesta en Caso de Pérdida de Personal Clave.
- ✓ CNTG-EJC-07 Procedimiento de Respuesta en Caso de Pérdida de Datos.

9.4.4. Equipo de Soporte Técnico

- **Objetivo**

Establecer una pauta de acción ante casos de contingencia que permita ordenar los esfuerzos de reacción y remediación con prontitud y eficacia.

- **Alcances**

  Dirigido a :

  Coordinador de Sistemas.
  Personal de Soporte Técnico externo a PERUPETRO S.A.

- **Responsabilidades**

  Este equipo estará integrado por el Coordinador de Sistemas y el Personal Externo de Soporte Técnico. Sus responsabilidades relativas al Plan de contingencia serán:

  - ✓ Determinar los equipos, software base u otros periféricos que han sido dañados.
  - ✓ Revisar la evaluación de prioridades del plan y revisar qué aplicaciones son críticas y cuáles no, así como determinar quién es responsable de cada una de ellas y contactarlos.
  - ✓ Ejecutar los procedimientos necesarios para trasladar los equipos a un nuevo ambiente y de ser necesarios, adquirir otros nuevos.
  - ✓ Ejecutar los procedimientos necesarios para restaurar el software y las aplicaciones, el hardware y los equipos de comunicaciones.

- **Procedimiento Ante una Contingencia**

  El Equipo de Soporte Técnico se encargará de ejecutar los procedimientos de la contingencia y

comunicar los resultados al Coordinador del Plan de Contingencia.

El Equipo de Soporte Técnico deberá coordinar directamente con los proveedores de equipos aplicando los procedimientos que se detallan a continuación

- ✓ CNTG-EJC-01 Procedimiento de Respuesta en Caso de Pérdida de Local Principal.
- ✓ CNTG-EJC-02 Procedimiento de Respuesta en Caso de Pérdida de Equipos Críticos.
- ✓ CNTG-EJC-03 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones de Voz.
- ✓ CNTG-EJC-04 Procedimiento de Respuesta en Caso de Pérdida de Comunicaciones de Datos.
- ✓ CNTG-EJC-05 Procedimiento de Respuesta en Caso de Pérdida de Software Base y Aplicaciones.
- ✓ CNTG-EJC-06 Procedimiento de Respuesta en Caso de Pérdida de Personal Clave.
- ✓ CNTG-EJC-07 Procedimiento de Respuesta en Caso de Pérdida de Datos.

10. AUDITORIA DEL PLAN DE CONTINGENCIA

A continuación se presentan procedimientos que podrán ser utilizados por PERUPETRO S.A., o los terceros en que decida delegar esta tarea, para la realización de la auditoria del Plan de Contingencia.

10.1. Plan de Pruebas del Plan de Contingencia

Se requieren de planes adecuados para respaldar recursos computacionales críticos y para la recuperación de los servicios del área de sistemas a efectuarse luego de interrupciones no previstas. Periódicamente, los escenarios de contingencia deberán ser simulados y el plan ejecutado para probar su exactitud y efectividad. Como mínimo la prueba comprenderá:

- Recolectar los tapes del lugar remoto alternativo y realizar un procedimiento de recuperación utilizando únicamente los archivos contenidos en estos tapes.
- Probar la operación con el equipo de respaldo mínimo especificado.
- Simular pérdida de archivos clave, programas y servicios y verificar si pueden ser recuperados de acuerdo al plan.
- Probar la operación con el personal mínimo especificado.

10.1.1. Realización de Pruebas del Plan

La idoneidad y efectividad del plan de contingencia y de recuperación de desastres deber ser probada periódicamente.

Indicadores:

- Verificación de la idoneidad y efectividad del plan de contingencia y de recuperación de desastres.

Procedimiento:

- Revisar la documentación de pruebas anteriores del plan de recuperación de desastres para verificar la idoneidad y frecuencia de pruebas.

- Revisar el proceso aceptado para probar el plan de recuperación de desastres para determinar la idoneidad de los niveles de autoridad y responsabilidad para garantizar esta aceptación.

- Participar en y observar los resultados de la prueba del plan de recuperación de desastres para determinar la idoneidad del procedimiento de prueba.

10.1.2. Programación de las Pruebas

A continuación se presenta un plan tentativo de realización de pruebas del plan de contingencia.

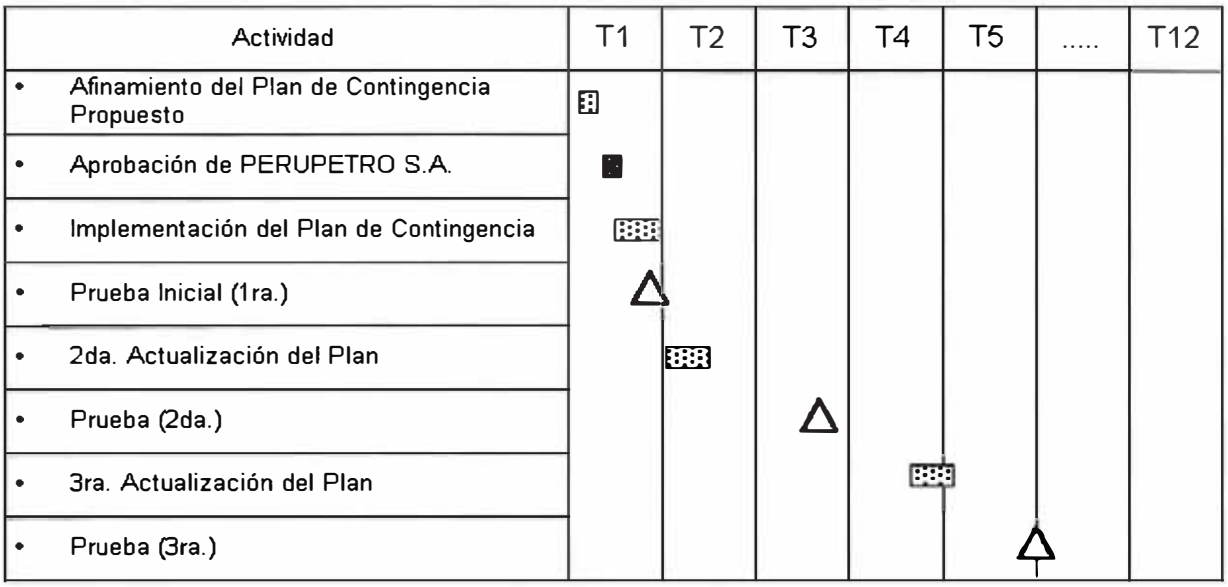


Gráfico Nro. 8 Programación de Pruebas.

10.2. Procedimientos mínimos de Auditoria del Plan de Contingencia

A continuación se presentan los Procedimientos mínimos de Auditoria del Plan de Contingencia:

10.2.1. Plan de recuperación

Objetivo:

Mantener un plan escrito y explícito para la operación de aplicaciones de misión crítica en la eventualidad de una falla mayor de equipos o software, o ante la temporal o permanente destrucción de las instalaciones.

Indicadores:

- Tiempo que transcurrirá entre la interrupción de los servicios del área de sistemas y el momento en que se restaure la operación de las funciones críticas del área.

Procedimiento:

- Evaluar el alcance y contenido del plan de recuperación de desastres del área de sistemas y determinar si copias del plan han sido ubicadas en lugares relevantes y distintos al de las oficinas de sistemas.

- Entrevistar a miembros seleccionados del área de sistemas (operaciones principalmente) para determinar su conocimiento y entendimiento del plan de recuperación de desastres.

- Discutir con el responsable la naturaleza y los procedimientos del plan de recuperación de desastres y los componentes del plan.

- Entrevistar a la jefatura de la División de Planeamiento para determinar el grado de compromiso en el proceso de planeamiento de la recuperación de desastres.

10.2.2. Aplicaciones de misión crítica

Objetivo

El plan de contingencia y de recuperación de desastres debe proveer prioridades para el restablecimiento de la

operación de aplicaciones de misión crítica o aplicaciones sensibles.

Indicadores

- Lista actualizada de las aplicaciones priorizadas según el orden en que deberán reponerse o activarse su operación.

- Tiempo que razonablemente se espera que transcurra antes que la operación normal de las operaciones se restablezca.

- Pérdida potencial de la organización si la operación de la aplicación no se restaura en un plazo apropiado.

- Etapa de un proceso normal cíclico en que podría interrumpirse.

Procedimiento

- Involucrar a los usuarios en la determinación de las prioridades a asignarse a las aplicaciones de misión crítica, así como a la secuencia en que se repondrá la operación de estas aplicaciones.

- Evaluar la secuencia de reposicion de operación desde el punto de vista de los procesos del negocio.

10.2.3. Recursos computacionales críticos

Objetivo:

El plan de contingencia y de recuperación de desastres debe identificar las aplicaciones de misión crítica, así como también los sistemas operativos y los archivos de datos requeridos para la reposición de la operación después que un desastre ocurra.

Indicadores:

- Lista de recursos computacionales críticos.

Procedimiento:

- Revisar la lista de recursos computacionales críticos y determinar si es razonable.

- Determinar si los archivos críticos están apropiadamente identificados en el plan de recuperación de desastres.

- Examinar el lugar de almacenamiento remoto y determinar si los medios magnéticos allí almacenados, contienen los archivos de datos, de aplicaciones y de software base requeridos, y si se encuentran apropiadamente actualizados.

10.2.4. Copias de Respaldo: lugar y equipos

Objetivo

El plan de contingencia y de recuperación de desastres debe incluir la provisión de un lugar de respaldo que cuente con el equipo computacional requerido para reponer las operaciones luego de que un desastre ocurra.

Indicadores

- Previsiones tomadas para contar con un lugar de respaldo (CPR) que cuente con el equipo computacional de respaldo (back-up computer) que se usará para restaurar y reponer las operaciones de sistemas después que un desastre ocurra.

Procedimiento

- Revisar el plan de recuperación de desastres del área de sistemas, para determinar las provisiones para contar con un lugar y equipo computacional de respaldo de ocurrir un desastre.

- Determinar si existe un procedimiento escrito para el uso de un lugar específico y equipamiento computacional específico para restaurar y reponer las operaciones de sistemas interrumpidas luego de un posible desastre, y asegurarse que los acuerdos realizados son razonables.

- Determinar el grado de compatibilidad entre el equipo computacional del área de sistemas y el que sería provisto como respaldo.

- Determinar si existirá suficiente tiempo y capacidad computacional de procesamiento en el lugar y equipos de respaldo, para reponer las operaciones del área de sistemas luego que ocurra un desastre.

- Determinar si se realizan pruebas periódicas del equipamiento computacional de respaldo que se planea utilizar para la reposición de las operaciones interrumpidas por un desastre.

- Entrevistar miembros seleccionados del área de sistemas para determinar su familiaridad con la operación de respaldo del equipo computacional y los procedimientos para reponer las operaciones luego de ocurrir un desastre.

10.2.5. Programación para operaciones de respaldo

Objetivo

Siempre que sea apropiado, el plan de contingencia y de recuperación de desastres debe proveer el personal técnico y de programación necesario para llevar a cabo las operaciones de respaldo del área de sistemas.

Indicadores

- Las políticas y procedimientos del plan de recuperación de desastres que incluyan al personal técnico y de programación requerido para operar y realizar los procedimientos y operaciones de respaldo de datos y sistemas.

Procedimiento

- Determinar el grado en que se ha requerido que el personal técnico y de programación intervenga para proveer capacidades especiales de programación o versiones de programas para las operaciones de respaldo.

- Revisar las provisiones del plan y los procedimientos establecidos para que el personal técnico y de programación logre restaurar la operación de los sistemas en los equipos computacionales de respaldo, y determinar las acciones tomadas para que el personal del área esté familiarizado con estos procedimientos.

- Seleccionar aplicaciones o módulos representativos en los que se ha identificado la necesidad de modificaciones antes de que puedan ser utilizados en los equipos de respaldo y probarlos a fin de determinar si las modificaciones se han realizado satisfactoriamente. Revisar la documentación sustentatoria de estas modificaciones para asegurar que estos programas de respaldo son los adecuados.

- Revisar los procedimientos del área de sistemas para asegurar que los programas de respaldo a ser usados en la reposición de las operaciones del área de sistemas después que ocurra un desastre, sean modificados adecuadamente cuando los programas de la operación normal se cambien.

10.2.6. Procedimientos de recuperación de archivos de datos

Objetivo

El área de sistemas debe establecer procedimientos para minimizar los requerimientos de recuperación de archivos de datos de respaldo después que un desastre ocurra.

Indicadores

Revisión de los procedimientos para minimizar los requerimientos de recuperación de archivos de datos de respaldo después que un desastre ocurra.

Procedimiento

- Determinar por observación qué procedimientos, incluyendo el copiado regular del contenido de los discos a cintas, cartuchos u otros medios magnéticos, son realizados rutinariamente por el encargado específico dentro del área de sistemas.

- Verificar que los archivos de respaldo son trasladados regularmente a un lugar de almacenamiento externo.

- Verificar que la documentación para aplicaciones de misión crítica, contengan procedimientos específicos de reconstrucción de datos.

- Determinar que existan procedimientos escritos para regenerar los archivos de sistemas (software base y similares).

- Verificar por observación que el lugar de almacenamiento externo tenga medidas adecuadas de protección y seguridad, para proteger los archivos y que existan reglas de retención y almacenamiento para asegurar datos actualizados para la recuperación de operaciones.

10.2.7. Pruebas del plan de recuperación de desastres

Objetivo

La idoneidad y efectividad del plan de contingencia y de recuperación de desastres deber ser probada periódicamente.

Indicadores

- Verificación de la idoneidad y efectividad del plan de contingencia y de recuperación de desastres.

Procedimiento:

- Revisar la documentación de pruebas anteriores del plan de recuperación de desastres para verificar la idoneidad y frecuencia de pruebas.

- Revisar el proceso aceptado para probar el plan de recuperación de desastres y determinar la idoneidad de los niveles de autoridad y responsabilidad para garantizar esta aceptación.

- Participar en las pruebas y observar y analizar sus resultados, para determinar la idoneidad de dichos procedimientos.

11. Conclusiones y Recomendaciones

11.1. Conclusiones

- Cualquier sistema o procedimiento que procese información importante y sensible, debe tener un Plan de Contingencias particular.

- La complejidad y profundidad de un Plan de Contingencias está directamente relacionada a la complejidad del sistema, su costo y su importancia en el cumplimiento de la misión de la organización.

- Los planes de contingencias no se deben concentrar en eventos límites o desastres, en detrimento del planeamiento de acciones menos catastróficas.

- El Plan de Contingencias de PERUPETRO S.A. puede ser utilizado por cualquier otra empresa como modelo pues las necesidades del Área de Sistemas se repiten en otra empresas.

- Analizando los casos de desastres sin Plan de Contingencias, se hace necesario asignar la importancia debida a las actividades de prevención pues estas, correctamente ejecutadas, disminuyen la probabilidad de ocurrencia de desastres.

- El tiempo máximo de espera para declarar a PERUPETRO S.A. en contingencia es de 12 horas mientras que el tiempo máximo de rehabilitación es de 24 horas, es decir, PERUPETRO S.A. puede

sobrevivir un (1) día sin sus procesos principales pues estos, por el tiempo máximo indicado, pueden ser ejecutados de por procesos manuales o pueden esperar hasta que se reestablezcan.

- Las pruebas de un Plan de Contingencias son necesarias para saber si las características usadas en su elaboración son las mismas.

- Si la empresa necesita un Centro de Procesamiento de Respaldo (CPR), éste debe cumplir con las características mínimas para proporcionar la seguridad exigida en estos casos.

- Cada empresa debe conocer sus procesos críticos y equipos indispensables para elaborar un correcto Plan de Contingencias.

- Es necesario una difusión correcta del Plan de Contingencias que permita, en caso desastres, actuar con la rapidez y eficacia necesaria para afrontar el problema.

11.2. Recomendaciones

- Toda empresa tiene sistemas o procedimientos importantes, por lo cual se recomienda tener un Plan de Contingencias particular.

- Cuando se elabora un Plan de Contingencias, se debe evitar el “sobre-planeamiento”, haciendo que el

Plan consista en la descripción de una serie de acciones orientadas a la recuperación del sistema en caso de desastres. Se recomienda no ser pesimistas ni optimistas, sino realistas.

- Se remienda usar la regla general siguiente: “Mientras más adverso sea el impacto de un evento (destrucción total del edificio por un terremoto, fuego o inundación) menor es la probabilidad de su ocurrencia”.

- Los planes deberán estar escritos y ser de conocimiento de todo el personal apropiado, así como ser probados periódicamente y actualizados según las necesidades si se desea que el plan sea efectivo y cumpla los objetivos trazados en su elaboración.

- El Plan de Contingencias de PERUPETRO S.A. puede ser utilizado por cualquier otra empresa como modelo pues las necesidades del Área de Sistemas se repiten en otra empresas. Se recomienda realizar ajustes al Plan para adecuarlo a los requerimientos específicos de cualquier empresa.

- Analizando los casos de desastres sin Plan de Contingencias, se hace necesario asignar la importancia debida a las actividades de prevención pues estas, correctamente ejecutadas, disminuyen la probabilidad de ocurrencia de desastres.

- Es necesario probar periódicamente el plan para conocer si los premisas o características principales al elaborarlo continúan vigentes o no. De no ser así, es necesario actualizarlo. Se recomienda una periodicidad de tres (3) meses para realizar las pruebas.

- El Centro de Procesamiento de Respaldo deberá estar disponible en las oficinas del proveedor del servicio los 365 días del año, siendo recomendable que el CPR no se encuentre a menos de 1 km. ni a más de 10 km. de la oficina principal de PERUPETRO S.A. para minimizar riesgos y optimizar los tiempos de traslado de operaciones e información.

- Cada empresa deberá elaborar un "Análisis de Impacto Económico", similar al Anexo Nro. 1 de este informe, para determinar los costos asociados a un desastre cuando se tiene o no un Plan de Contingencias. Asimismo, deberá definir sus procesos y equipos críticos, con el fin de tener claramente definido el plan de prevención o ejecución correcto.

12. Bibliografía

- "Plan Estratégico de PERUPETRO 2000-2005"
  Autor: PERUPETRO S.A.
  Año: 2000

- "Plan de Contingencias de PERUPETRO S.A."
  Autor: PERUPETRO S.A.
  Año: 2000

- "Plan de Contingencias y Seguridad de la Información"
  Autor: Instituto Nacional de Estadísticas e Informática INEI
  Año: 1997

- "Seguridad y Plan de Contingencias en Centros de Informática"
  Autor: Carmen Rosa Peña Enciso
  Informe Técnico para obtener el Título Profesional de Ingeniero Industrial
  Año: 1995