

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



DIPLOMADO EN AUDITORÍA INFORMÁTICA

Tema de Tesis:

Plan de Continuidad de Negocios – AGRIPAC S.A.

Tutor: Ing. Jorge Ugarte

Integrantes:

Ing. Alexis Luna
Ing. Natalia Rosado
Ing. Marcela Sánchez
Ing. Bolívar Vallejo

Noviembre - 2005

Guayaquil-Ecuador

Plan de Continuidad de Negocios AGRIPAC S.A.

Hoja de Control del Documento

Versión: 1.0

Ubicación del Plan: La impresión original del documento se encuentra en el casillero del Banco Bolivariano y cada uno de los integrantes del comité de Contingencias conservan copias del mismo. Además se mantiene el archivo en poder del Gerente de Sistemas.

Aprobación:

Noviembre - 2005

Guayaquil-Ecuador

INDICE

1. ANTECEDENTES
 2. OBJETIVOS
 3. ALCANCE
 4. METODOLOGÍA
 5. PLAN DE ACTIVIDADES
 6. INFORMACIÓN DE LA ORGANIZACIÓN
 - 6.1 Introducción
 - 6.2 Organigrama
 - 6.3 Información del Ambiente de Sistemas
 - 6.4 Administración y Control de IT
 - 6.5 Roles y Responsabilidades
 - 6.6 Infraestructura Técnica
 - 6.7 Aplicaciones
 7. ANÁLISIS DE RIESGO
 - 7.1 Antecedentes
 - 7.2 Análisis de Riesgos
 - 7.2.1 Análisis de los riesgos determinados para el Área del Negocio en General
 - 7.2.2 Análisis de los riesgos determinados para el Área de Sistemas
 - 7.2.3 Conclusión
 8. ANÁLISIS DE IMPACTO DE NEGOCIOS
 - 8.1 Análisis de Impacto
 - 8.2 Aplicaciones Críticas
 - 8.3 Tiempo de Recuperación
 - 8.4 Conclusión
 9. CRITERIOS PARA LA DECLARACIÓN DE CONTINGENCIA Y ACTIVACIÓN DEL CENTRO ALTERNO
 - 9.1 Fases del Plan de Acción
 - 9.2 Estructura Organizativa para la Recuperación
 10. EQUIPOS DE TRABAJO RESPONSABILIDADES
 - 10.1 Comité de Contingencia
 - 10.2 Equipo de RR. HH.
 - 10.3 Equipo de Comunicaciones
 - 10.4 Equipo de Logística
 - 10.5 Equipo de Infraestructura
 - 10.6 Equipo de Procesos
 - 10.7 Coordinador de Tecnología
 - 10.8 Equipo de Administración de Ambientes
 - 10.9 Equipo de Soporte
 11. ESCENARIOS
 12. ESTRATEGIAS DE RECUPERACIÓN
 - 12.1 Alternativas de Recuperación
 - 12.2 Situación Actual
 - 12.3 Análisis de Impacto Financiero
 - 12.4 Selección y Desarrollo de Estrategia
 13. ESQUEMA DE PRESTACIÓN DE SERVICIOS EN CONTINGENCIA
 14. ENFRENTANDO LA CONTINGENCIA
 15. PLAN DE ACTIVIDADES DURANTE LA CONTINGENCIA
 16. PLAN DE NORMALIZACIÓN DE SERVICIOS LUEGO DE LA CONTINGENCIA
 - 16.1 Evaluación de Resultados
 - 16.2 Retroalimentación del Plan de Acción
 17. ADMINISTRACIÓN Y MANTENIMIENTO DEL PLAN DE CONTINGENCIA
- ANEXOS**

Directorio de Miembros del Equipo de recuperación
Recursos Mínimos de Recuperación
Directorio de Proveedores
Diagrama y Configuración de Comunicaciones
Procesos Alternos Manuales
Procedimientos de recuperación

1. ANTECEDENTES

Un Plan de Continuidad de Negocios es un proceso enfocado en reducir riesgos que ocasionen problemas en las operaciones normales de una organización. Para salvaguardar que el nivel de impacto de estos posibles incidentes no ocasionen la inoperatividad de los procesos considerados críticos e identificar los recursos alternativos.

Los estudiantes del Diplomado de Auditoria Informática realizamos una consultoría sobre Plan de Continuidad de Negocios cuyo resultado servirá como base para su posterior implantación en "AGRIPAC S.A." y sobre la cual basamos el presente Plan aplicable ante una posible amenaza de desastre de los riesgos más relevantes detectados dentro del Análisis de Impacto realizado.

Debido a estos antecedentes AGRIPAC S.A. requiere mantener la continuidad de sus operaciones desde Balanfarina – Km. 6 ½ vía Duran Tambo donde se ubicaría el Centro Alterno y Centro de Ingreso de Datos.

Este plan considera los pasos a ser ejecutados por la organización en caso de que se presente un desastre que afecte la normal operatividad del Centro de Computo Principal. Cabe recalcar, que la importancia de este documento radica en la difusión y compromiso de todos quienes forman parte del Equipo de Contingencia, por tanto el papel que desempeñen cada uno de sus miembros en el momento indicado podrá garantizar que este Plan cumpla con sus Objetivos.

2. OBJETIVOS

Los objetivos del Plan de Contingencia son:

1. Precautelar la seguridad física de los empleados
2. Mantener el control de los servicios que presta el Centro de Cómputo en modalidad de Contingencia, la cual estará a cargo de Ing. Bolívar Vallejo.
3. Organizar los grupos de personas responsables por la operación en contingencia, la coordinación y control y las actividades necesarias para recuperar el servicio pasada la contingencia.
4. Precautelar los activos tecnológicos, de información y conectividad.
5. Identificar y documentar las actividades, procedimientos y tareas necesarias para las operaciones en contingencia y la posterior normalización de los mismos.
6. Identificar, dimensionar y organizar los recursos necesarios para las operaciones en contingencia en un site provisional.

3. ALCANCE

Este Plan incluye la activación de un Centro Alterno que permite la recuperación de los procesos críticos del negocio soportados fuertemente por IT.

Las Aplicaciones a recuperar que soportan estos servicios vitales, son las siguientes:

- Aplicación ELITE
 - Módulo de Producción
 - Módulo de Facturación
 - Módulo de Abastecimiento
 - Módulo de Inventario
 - Módulo de Crédito y Cobranzas

Existen diferencias sustanciales entre un Plan de Contingencia y un Plan de Emergencia. En este documento se encontrarán procedimientos propios de un Plan de Emergencia para la recuperación de operaciones de los servicios de Procesamiento del Centro de Cómputo de AGRIPAC S.A. Por lo tanto, este documento no incluye los procedimientos para la respuesta a incidentes ya que la empresa AGRIPAC cuenta con un Plan de Respuesta a Crisis que incluye procedimientos de seguridad que salvaguardan la integridad física de las instalaciones de la organización, y/o de sus ocupantes, tales como: extinción de incendios, evacuación y desalojo, amenazas de bomba, actos hostiles entre otros.

Dentro de este documento no se incluye el Plan de Pruebas, Capacitación e Implementación, ni el Plan de Auditoria.

4. METODOLOGÍA

El Plan de Contingencia describe los pasos necesarios para poder asegurar que no sean afectadas las Operaciones consideradas estratégicas por cualquier incidente considerado como desastre.

Cada proceso soportado fuertemente por Tecnología fue considerado para ser analizado y se determinaron que aspectos podrían ser eventos riesgosos para fallos del sistema. Dentro de la Metodología de uso se ha considerado los objetivos de COBIT relacionados directamente a la Continuidad de los Negocios.

Las posibles fallas fueron identificadas y en base a ellas se estableció un tiempo máximo de recuperación y la probabilidad de que estas se presenten, tanto la duración como la probabilidad han sido usados para establecer una valoración del riesgo.

Los cambios tecnológicos que surgen a través del tiempo ocasionan variaciones dentro de las prioridades establecidas en los riesgos, por tanto este Plan es un documento dinámico, que debe ser actualizado periódicamente para que reflejen los nuevos cambios relacionados al manejo y control de la información.

5, PLAN DE ACTIVIDADES

Para efectos del desarrollo de este Plan se ha elaborado un Plan de Actividades , que cubre con todos los aspectos tratados dentro del contenido del mismo, a continuación se adjunta la Tabla con la secuencia de actividades, descripción y sus responsables.

ACTIVIDADES	ESTADO	RESPONSABLE
Reconocimiento del Marco General de Negocio		
Identificar los Objetivos del Negocio	Listo	Cesar Vallejo
Identificar los Procesos Críticos del Negocio	Listo	Todos
Planificación del Proyecto		
Definición de proyecto	Listo	Todos
Establecer Objetivos de Proyecto	Listo	Todos
Definir el Alcance del Proyecto	Listo	Todos
Determinar los recursos necesarios	Listo	Todos
Establecer Responsabilidades	Listo	Todos
Elaborar Plan de Actividades	Listo	Todos
Análisis del Entorno		
Revisar Estructura de la Organización	Listo	Cesar Vallejo
Revisar Plan Estratégico de la Organización	Listo	Cesar Vallejo
Revisar Estructura del Area de IT	Listo	Marcela Sánchez
Revisar el Plan Estratégico del Area de IT	Listo	Marcela Sánchez
Revisar el Manual de Funciones	Listo	Natalia Rosado
Identificar las Políticas o Procedimientos del Área de IT	Listo	Natalia Rosado
Identificar la Infraestructura Tecnológica del Area de IT	Listo	Alexis Luna
Identificar las Aplicaciones y ambiente requerido	Listo	Alexis Luna
Análisis de Impacto del Negocio		
Identificar los procesos críticos del negocio	Listo	Marcela Sánchez/Cesar Vallejo
Análisis de Riesgos que impacten los procesos críticos	Listo	Natalia Rosado
Conclusiones de BIA		Marcela Sánchez
Creación del Plan de Continuidad del Negocio		
Determinar la organización por contingencia	Listo	Marcela Sánchez
Determinar el alcance de cada servicio durante la contingencia	Listo	Alexis Luna
Determinar los escenarios de contingencia	Listo	Alexis Luna
Identificar y priorizar los elementos críticos por servicio necesarios para operar durante la contingencia (recursos tecnológicos, de información, materiales, humanos, etc.)	Listo	Alexis Luna/Cesar Vallejo
Determinar el modelo de operación de cada servicio durante la contingencia (grupos, responsabilidades, procedimientos, soportes, cronogramas, etc)	Listo	Alexis Luna
Determinar de equipos/responsabilidades de contingencia	Listo	Marcela Sánchez
Control y seguimiento durante la contingencia	Listo	Natalia Rosado
Plan de normalización de los servicios luego de la contingencia	Listo	Natalia Rosado
Documentación		
Estructurar Documentación	Listo	Marcela Sánchez
Elaborar Diapositivas de Presentación Final	Listo	Todos
Presentación de la documentación BCP	Listo	Todos
Sustentación de Proyecto	Listo	Todos

6. INFORMACIÓN DE LA ORGANIZACIÓN

6.1 Introducción

Agripac S.A. es una de las empresas del Grupo Corporativo Agroindustrial AGRIPAC S.A. que importa, fabrica, distribuye y comercializa productos para la agricultura, balanceado, alimentos para avícolas, ganado y acuicultura, que cuenta actualmente con 125 sucursales ubicadas en las diferentes provincias del país.

El empresa cuenta con diversas líneas de productos las cuales a continuación se detalla:

- **La División AGRÍCOLA de AGRIPAC** es el líder del mercado ecuatoriano en importación y distribución de insumos agrícolas; y el segundo proveedor más importante de fertilizantes.

Más de 110 almacenes y personal técnico y comercial de primer nivel desplegados en todo el país, garantizan un abastecimiento oportuno y asesoramiento permanente. Además, la calidad de nuestros productos permiten un apropiado manejo del cultivo, desde el proceso de preparación de suelos, hasta la cosecha y pos cosecha.

La clave de éxito es mantener el contacto directo con el cliente, para dar un servicio integral: desde asesoría en el cultivo, hasta las posibilidades de comercialización de su producción. Son los principales proveedores de insumos agrícolas para los cultivos de mayor importancia económica en el país, como banano, flores, arroz, papa, maíz, palma, hortalizas y otros. Principales productos: Fungicidas – Herbicidas – Insecticidas/Acaricidas – Nematicidas – Abonos Foliares y Fertilizantes Edáficos – Bioestimulantes – Bombas y motosierras – Fijadores/Ceras – Reguladores de pH.

- **La División ACUACULTURA de AGRIPAC**, es el principal proveedor de insumos acuícolas en todo el país. Contribuyen con la industria ofreciendo una gama completa de productos de altísima calidad, para todas las especies y etapas del cultivo.

La clave de éxito es mejorar constantemente la productividad de los cultivos acuícolas, a través de la calidad de nuestros productos y el respaldo técnico oportuno y eficiente, en cualquier punto de venta del país.

El prestigio de sus marcas, la más grande cadena de distribución en todo el Ecuador y la Infraestructura industrial con tecnología de punta, le permite liderar ampliamente este mercado. Principales productos: Balanceados – Fertilizantes – Desinfectantes – Antibióticos – Prebióticos – Enriquecedores – Suplementos Alimenticios, Antivirales – Dietas para laboratorios de larvas – Aditivos.

- **La División SEMILLAS de AGRIPAC**, es el más grande proveedor de semillas de granos, vegetales y pastos en Ecuador. Ofrecemos al agricultor la más amplia variedad de semillas en todo el país, las que cumplen con las expectativas más exigentes de calidad y rendimiento. Además, la venta está respaldada con programas permanentes de ensayos e investigaciones técnicas, con un equipo

profesional de primera categoría, y con vasta experiencia en cada uno de los cultivos.

La infraestructura del Grupo nos permite establecer un círculo de negocio de enorme beneficio para la producción mediante un proceso que va desde la provisión de semilla, el asesoramiento del cultivo, cosecha, comercialización y procesamiento de la misma, beneficiando así, a toda la cadena de producción.

Principales productos: Maíz, Arroz, Soya, Pastos, Sandía, Tomate, Brócoli y las demás hortalizas sembradas en el Ecuador.

- **La División ANIMAL de AGRIPAC**, cuenta con el portafolio de productos veterinarios más completo del país y son los líderes en la distribución directa de marcas de prestigio internacional.

Desarrollamos programas de desinfección y bioseguridad para todas las especies animales de importancia económica.

Además de ofrecer el mejor servicio, nuestra infraestructura y personal técnico de primer nivel, permiten desarrollar fórmulas de alimentos concentrados que cumplan con las exigencias internacionales de calidad, a fin de satisfacer todos los requerimientos nutricionales de las especies tratadas.

Principales productos: Balanceados – Medicamentos y Medicinas – Vitaminas – Desinfectantes – Productos para Bioseguridad – Aditivos y Microelementos.

- **La División CONSUMO de AGRIPAC**, ofrece productos altamente eficaces para el control de plagas tanto a nivel de hogares como de industrias y son líderes en líneas de insecticidas domésticos.

Dirigida por un equipo de técnicos altamente capacitados, esta División ofrece soluciones integrales para mejorar la salubridad de la comunidad y aportar con tecnología de punta al cuidado del ambiente.

Cuentan con las marcas de mayor prestigio en alimentos para mascotas y a través de su propia cadena de distribución, son los primeros en estos mercados.

Principales productos: Alimentos para mascotas – Insecticidas, Raticidas y otros Plaguicidas de uso doméstico – Accesorios varios.

- **BALANFARINA S.A.** dedicada a la industria de alimentos balanceados desde 1979. Es una empresa pionera en esta actividad y se perfila como una de las industrias de mayor crecimiento.

Cuenta con una infraestructura diseñada con la más alta tecnología y con una capacidad de producción combinada de más de 15TM por hora, a fin de satisfacer la demanda de balanceados en mercados de enorme importancia económica como el camaronero, veterinario, avícola, ganadero y otros, en todo el país.

Es parte del Grupo Corporativo AGRIPAC desde el 2002 y esto garantiza no sólo la mejor calidad en los productos balanceados, sino además, el respaldo técnico altamente calificado y la infraestructura logística ya

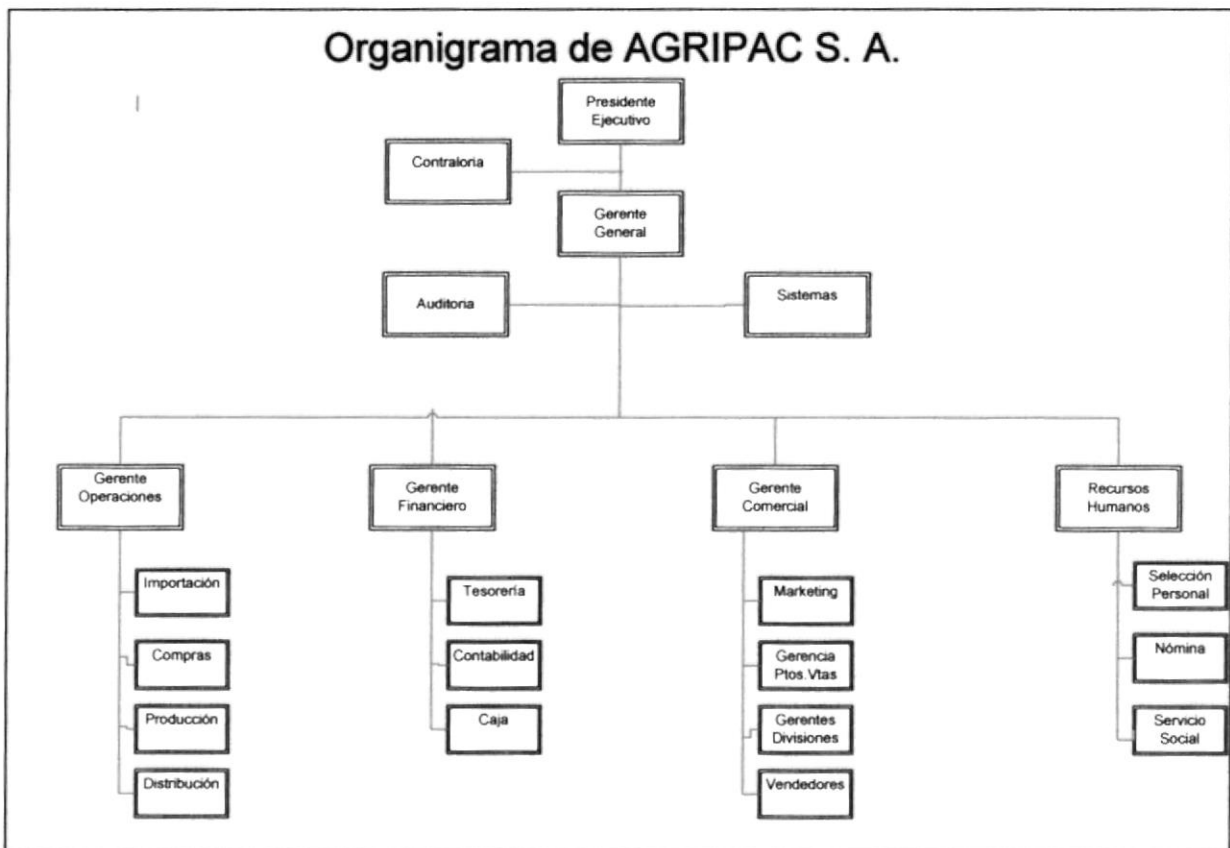
reconocida en todo el Ecuador. Produce balanceados para pollos, agnado, cerdos, camarón y otras especies menores.

La empresa tiene una participación en el mercado que la consolida como una de las empresas más importante del país, aspira alcanzar el 40 % del mercado. Su volumen de transacciones es aproximadamente de 4 millones mensuales. Cuenta en su estructura organizacional con 700 empleados a nivel nacional y su facturación está estimada en 100 millones de dólares anuales.

La organización depende en alto grado de la tecnología y de la información para su operación, el departamento de sistemas brinda servicios a todas las áreas del negocio, cuenta con una red local a la que se conectan ciento cincuenta usuarios. La información crítica del negocio es llevada en una aplicación centralizada que cubre todas las áreas de la empresa.

La preocupación de la gerencia se basa en la seguridad de la información y en el uso y acceso que tienen los usuarios a los diferentes aplicativos que se encuentran en producción, así como el adecuado funcionamiento de los diferentes procesos que garantizan la continuidad del negocio.

6.2 Organigrama



6.3 Información del Ambiente de Sistemas

AGRIPAC S. A. actualmente cuenta con varias líneas de negocio que son soportadas por las diferentes unidades de la organización, entre ellas podemos destacar:

UNIDADES DE NEGOCIO:

- Oficina Matriz (120 usuarios)
- 3 Plantas de Producción: Pascuales-Quito-Riobamba (óo usuarios)
- 20 Sub-centros de Abastecimiento
- 105 Puntos de Ventas Remotos

La organización depende en alto grado de la tecnología para el desarrollo y control de sus operaciones de: Producción, Abastecimiento, Compras y Ventas, el procesamiento y control de la información está centralizado y soportado por la siguiente infraestructura tecnológica:

En el Centro de Cómputo en Matriz de Agripac S.A. se consta con dos divisiones:

- ❖ División desarrollo de Sistemas.
- ❖ División de producción de Sistemas.

6.4 Administración y Control de IT

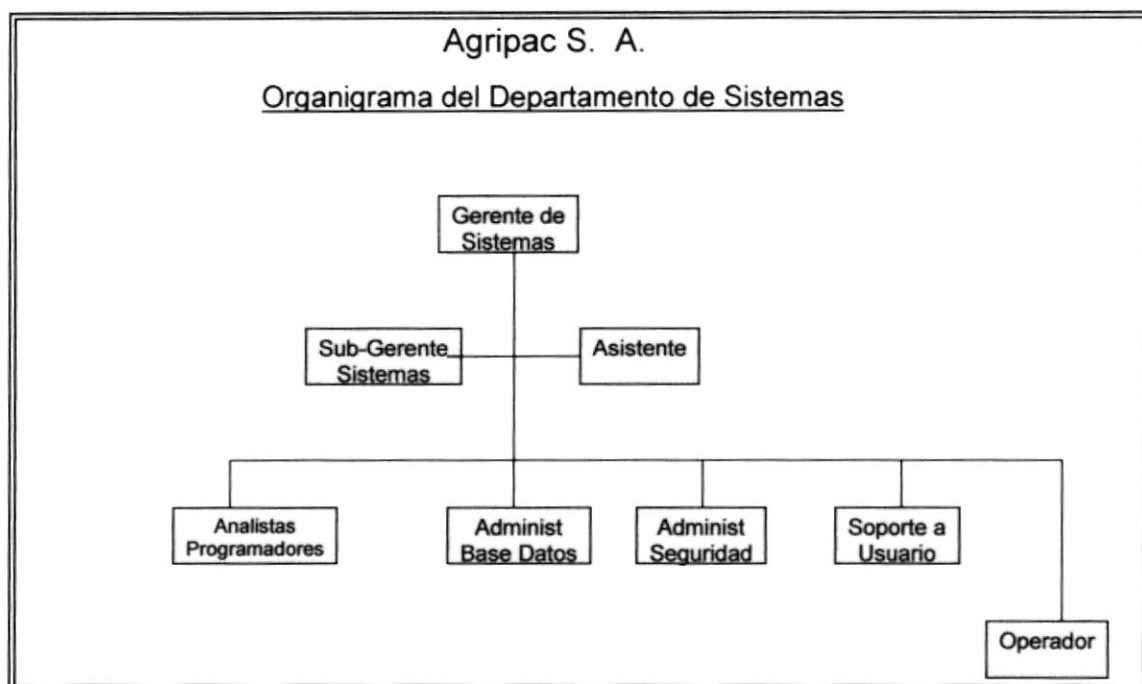
El departamento de Sistemas de Agripac S.A. tiene como estrategia fundamental proveer a la organización los recursos tecnológicos necesarios distribuidos y utilizados eficientemente para brindar a todas las unidades de la organización información efectiva, oportuna y confiable.

Para una mejora administración y control de IT, el departamento de sistemas mantiene una política de seguridad, actualmente posee procedimientos, planes formalmente establecidos como:

- ❖ Políticas de Seguridad de redes y del centro de cómputo
- ❖ Procedimiento para compra de hardware y software
- ❖ Procedimiento para atención de requerimientos de usuarios
- ❖ Procedimiento para desarrollo y mantenimiento de aplicación
- ❖ Procedimiento para apertura, mantenimiento y baja de cuentas de usuarios
- ❖ Procedimiento de respaldo de información
- ❖ Procedimientos de seguridad de bases de datos

El departamento de sistemas es el encargado de brindar el servicio a todas las áreas del negocio, el equipo de sistemas está conformado por 11 personas:

- 1 Gerente de Sistemas,
- 1 Responsable del ambiente de Producción,
- 1 Responsable del ambiente de Desarrollo
- 1 Administrador de la Base de Datos
- 1 Administrador de la Red
- 3 Analistas Programadores,
- 2 Técnicos de Hardware y Software
- 1 Asistente de gerencia,



6.5 Roles y responsabilidades:

- ❖ **Gerente de Sistemas.-** Proveer a la organización de unos Sistemas de Información IT que esté alineado con los objetivos del negocio. Elaborar el plan estratégico de Sistemas de Información IT y de Comunicaciones; Planificar, liderar y coordinar la ejecución de nuevos proyectos de sistemas y comunicaciones, asesorar a la gerencia general en la toma de decisiones para la inversión de nuevas tecnologías (Hardware/Software), administrar los recursos tecnológicos de la organización optimizando su utilización.
- ❖ **Jefe Desarrollo.-** Dirigir, desarrollar y controlar que los proyectos definidos se realicen dentro de los plazos establecidos en el cronograma de trabajo.
- ❖ **Jefe de Producción.-** Planear, organizar, dirigir, controlar y coordinar las actividades que cumplen las áreas de operación, entrada y salida de datos, centro de control de red, Bases de Datos e infraestructura Tecnológica.
- ❖ **Administrador de la Base de Datos.-** Controlar que todas las aplicaciones estén acordes con la arquitectura de datos de la entidad.
- ❖ **Administrador de la Red.-** Garantizar la seguridad, integridad, confidencialidad y disponibilidad de los servicios de mensajería y acceso a la información de la red de la organización. Coordinar con el Gerente de Sistemas los requerimientos y políticas, que garanticen el buen funcionamiento de la red.
- ❖ **Analistas de Sistemas.-** Coordinar con la Gerencia de Sistemas la planificación, análisis y desarrollo de nuevos proyectos de sistemas de información IT, generando un servicio informático que garantice información veraz y oportuna a todo nivel organizacional.
- ❖ **Técnicos de Hardware y Software.-** Apoyo a los usuarios finales con las dificultades de Hardware y Software, entrenamiento a usuarios para buen uso de Hardware y Software. Corrección de problemas de usuarios finales en la aplicación principal y configuraciones de equipos de comunicación.

- ❖ **Asistente de Gerencia.-** Actividades de administración de papelería enviada y recibida, elaboración de comunicaciones internas de la gerencia de sistemas al personal de IT, administración de agenda interna y externa del gerente de sistemas.

6.6 Infraestructura técnica

En el mismo centro de cómputo se posee:

5 Servidores (Intel)

- 2 Mensajería (Plataforma Microsoft)

- 3 Aplicativos (Producción, Desarrollo y Backup)

Sistema Operativo UNIX

Base de Datos Informix

Sistema aplicativo integrado ELITE (13 módulos)

Acceso a Internet mediante ancho de banda de 256 Kbps.

La organización cuenta con las siguientes redes:

Una red local conformada por 120 usuarios, tres redes remotas vía satelital y micro ondas (Plantas), 20 enlaces punto a punto (sub-centros) y ciento cinco puntos de ventas que se conectan mediante acceso remoto vía dial up. La información crítica del negocio es llevada en la aplicación centralizada ELITE que cubre todas las áreas de la empresa.

La seguridad y acceso lógico a la red es controlada a través de un Firewall ISA SERVER, el control de virus y filtración de la mensajería se lo hace con el MAIL SCAN a nivel de servidor y con el F-PROT Profesional en las estaciones de trabajo. Los accesos físicos y lógicos están regulados por políticas y procedimientos que deben ser observados por todos los miembros de la organización.

Ver en los anexos adjuntados el Diagrama de Red.

6.7 Aplicaciones

La organización cuenta con una aplicación multiempresa integrada (ERP) llamada elite la que está compuesta de 13 módulos que soportan las diferentes áreas, la aplicación está desarrollada en 4GL para Informix fue adquirida a un proveedor canadiense la empresa adquirió los códigos fuentes, el mantenimiento está a cargo del equipo de sistemas, los módulos que contiene la aplicación son los siguientes:

Módulo de administración y Seguridad

Módulo de Contabilidad

Módulo de Compras

Módulo de Importaciones

Módulo de manejo de Inventario

Módulo de Producción

Módulo de Ventas

Módulo de Distribución

Módulo de Finanzas y Cuentas por Pagar

Módulo de Cuentas por Cobrar

Módulo de Activo Fijos

Módulo de Análisis de Ventas

Módulo de Presupuesto

Las tres plantas de producción y los veinte sub. centros realizan su labor directamente en la aplicación central a través varios tipos de enlaces punto a punto (satelital y micro ondas), los puntos de ventas cuentan con una aplicación para facturación, control de inventario y cuentas por cobrar que está desarrollada en cobol, el mantenimiento es realizado por el departamento de sistemas, las transacciones son enviadas diariamente vía módem a la oficina central donde mediante una interfase es integrada a la aplicación central (elite). El módulo de nómina está desarrollada en Visual Basic trabaja en línea y se integra a la aplicación central mediante interfase.

7. ANÁLISIS DE RIESGO

7.1 Antecedentes

Agripac S.A., dedicado a la comercialización de insumos agrícolas, consta de varios procesos de los cuales se han determinado como críticos y directamente vinculados al área de sistemas los procesos de:

- **Facturación**
- **Abastecimiento**
- **Crédito y Cobranzas**
- **Producción**
- **Inventario**

Operación

- **Pólizas de Seguros.**

Agripac S.A. mantiene una relación muy estrecha con la compañía de Seguros Sucre, ya que funciona como broker de esta compañía. Aprovechándose de esto, tiene la totalidad de sus activos asegurados: Edificios, mercadería, equipos de cómputo, etc y pólizas de de vida para el personal. El área tecnológica también se encuentra asegurada ya que cuenta con un Valor de Rescate por Recuperación de Información que, en caso de pérdidas, sería utilizado para contratación de personal adicional necesario, gastos de recuperación, etc. Además cuenta con un seguro que cubre parcialmente pérdidas por fraude o robo. *[Anexo de Pólizas de Seguro]*

- **Puntos de Venta**

Todos los puntos de venta cuentan con un sistema aplicativo de facturación, manejo de clientes e inventario denominado DOS y que trabaja sobre Windows.

Existen 125 agencias sobre el territorio nacional, de éstas, 20 se conectadas en línea con el sistema centralizado Elite, pero en caso de Contingencia, usan DOS para poder seguir con la facturación. En caso de no contar con energía eléctrica o con la aplicación DOS, todos cuentan con un procedimiento manual para su facturación.

El sistema DOS se actualiza 3 veces por semana con información de clientes (cupos de crédito, cartera vencida, etc.). El inventario se maneja individualmente en cada punto de venta. La actualización desde Guayaquil se realiza vía módem o por medios magnéticos enviados en valija a los puntos de venta que no están en línea. De la misma manera, estas agencias envían diariamente la información a Guayaquil, donde se ejecuta un proceso batch de una interfaz con Elite que actualiza los datos de ventas, cartera, pedidos, etc.

Desde Guayaquil se transfiere la información hacia las agencias de la costa, centro del país, y Quito. Y desde Quito se encargan de enviar a su vez a las provincias del norte y Oriente.

- **Enlace de Telecomunicaciones entre Guayaquil y filiales**

Desde Guayaquil hay un enlace Frame-Relay, proporcionado por Porta, hacia Quevedo, desde donde se reparte en forma de estrella a otro grupo de agencias *[Gráfico Fase I y Fase II]*. Actualmente, si se cae el enlace, se pierde la comunicación con estos puntos, es por esto que se está implementando un enlace redundante que conecta Guayaquil con Pascuales – Nobol – Daule, y llega hasta Quevedo y los demás puntos. Este contrato es con Iseyko, quienes nos proporcionan la mayoría de los enlaces de red, convirtiéndose así en nuestro mayor proveedor de Comunicaciones. *[Anexo contrato Iseyko]*.

El contrato con Iseyko incluye la garantía del enlace de 256 Kbps y el mejoramiento continuo del servicio. A propósito de esto, Agripac les sugirió adquirir un equipo de monitoreo del enlace para que estén siempre atentos de las posibles caídas del servicio y puedan actuar con antelación.

Además, la compañía tiene un acuerdo con Iseyko para contar con un equipo adicional en caso de que alguno falle en un punto de venta, de esta manera, el riesgo en los enlaces de corto alcance se minimiza trabajando de la siguiente manera: El proveedor tiene un equipo localizado estratégicamente en Quevedo (punto central) donde se encuentra una persona capacitada para instalarlo en cualquier agencia cercana donde haya surgido el daño. La idea es acortar el tiempo de recuperación de la señal en vez de esperar algunas horas de viaje de un técnico del Iseyko que pueda solucionar el problema.

- **Facturación de Puntos de venta**

El número de factura lo imprime el sistema, no viene pre-impreso. Esto está autorizado por el SRI. El sistema DOS permite modificar la secuencia del número de factura en los casos en que se requiere.

- **Central Telefónica y Enlaces de Voz**

La Central Telefónica de la Empresa es administrada por el Departamento de Sistemas. Se cuenta con 90 líneas convencionales. La empresa también cuenta con enlaces de voz con los puntos de venta que están en línea. El proveedor de los enlaces de voz es Iseyko. Este enlace conecta a Guayaquil con las demás agencias resultando la manera más fácil y económica de comunicarse. Si el proveedor falla con el servicio, se incurriría en gastos de comunicación mayores y afectaría el tiempo de actualización del sistema DOS.

- **Producción**

La producción se efectúa en 3 plantas principales que representan el 80% de producción de Agripac: Las Plantas de Pascuales y Quito que pertenecen a Agripac S.A., y Balanfarina que funciona como proveedor de Agripac.

La Planta Pascuales procesa todos los productos líquidos y la Planta de Quito produce artículos sólidos y en polvo debido a la facilidad que brinda su clima. Balanfarina produce balanceados, y es administrado de manera independiente, pero su único cliente es Agripac S.A..

Todas las fábricas cumplen con estrictas normas ambientales, de salud y de seguridad industrial. La planta Pascuales se encuentra certificada bajo la norma ISO 14000.

Cada planta tiene enlace directo con Guayaquil, conectados en línea con Elite. El proceso de fabricación se encuentra automatizado en un alto porcentaje, ya que es en este sistema donde se manejan fórmulas de producción, y todos los componentes de costos, etc.

El enlace con las fábricas es redundante y se cuenta con equipos de alta velocidad de 10 Mb. En las plantas el diseño de la red se basa en subredes. La planta de Pascuales cuenta con 18 usuarios, Quito con 16 y Balanfarina con 33.

La planta de Quito cuenta con PERIBIT, que es una herramienta para administrar y optimizar el ancho de banda.

- **Energía Eléctrica**

Todas las plantas y la oficina principal tienen su propio generador de energía los que se encuentran preparados para funcionar en el momento que se produce

un corte del servicio eléctrico público, a estos generadores se les realiza un constante mantenimiento y hay un responsable de mantener el combustible necesario para 8 horas de funcionamiento.

- **Instalaciones de la Matriz**

En el edificio de la matriz Guayaquil funciona el Consulado de Inglaterra y se han suscitado leves intentos terroristas en algunas ocasiones. A partir de estos eventos, se instalaron sistemas de seguridad y monitoreo.

- **Internet / Control de Virus**

El número de usuarios en la red es de 207. De estos, 50 usuarios tienen internet, y 20 de ellos tienen acceso restringido.

Para protección de virus, el servidor de Mensajería tiene instalado Mail Scan y F-Prot para las estaciones de trabajo. Este antivirus se actualiza en línea. No se han presentado casos de virus.

Además la empresa tiene instalado Microsoft ISA Server como firewall para evitar la exposición a terceros de información confidencial y controlar los accesos externos no autorizados a la red LAN y WAN de la Compañía a través del enlace a Internet.

Cabe recalcar también que el servidor principal trabaja sobre Unix, que es un sistema operativo muy fuerte y casi inmune ante eventualidades frecuentes de virus.

7.2 Análisis de Riesgos

El análisis de riesgo valora la posibilidad de que se produzca un daño que afecte a los activos de la empresa. En el contexto de un Plan de Continuidad de Negocio, el Análisis de Riesgos debe valorar los elementos que soportan a los procesos esenciales y los diversos riesgos que les pueden afectar: intencionados, negligencias o eventos naturales. Entre los riesgos más significativos y que afectarían al negocio en general, hemos encontrado los siguientes:

Riesgos Intencionales
Robo de Equipos
Alteración o daño de información por ataque de Virus / Hackers
Ataques terroristas / Amotinamiento de civiles
Riesgos por Negligencia o Servicio esperado no Proporcionado
Errores Humanos / Falta de capacitación de Personal (interno y externo)
Falla en el Servicio de Telecomunicaciones
Falla en el Servicio de Energía Eléctrica
Evasión de Impuestos / Información tributaria errónea. Problemas con SRI
Daño de Instalaciones de Servicios básicos
Incumplimiento de Normas Ambientales y de Salud
Riesgos por Desastres Naturales
Incendios
Terremotos
Tormentas eléctricas

7.2.1 Análisis de los riesgos determinados para el Área del Negocio en General

Leyenda	Probabilidad	Impacto
Muy baja	2	1
Baja	4	3
Alta	6	5
Muy alta	8	7

Riesgo asociado al Negocio en general	Control	Ha Ocurrido	Probabilidad	Impacto	Severidad
Riesgos Intencionales					
Robo de Equipos	s	s	2	5	10
Ataque de Virus / Hackers	s	n	4	7	28
Ataques terroristas	n	s	6	6	36
Fraudes	s	s	4	4	16
Riesgos por Negligencia o Servicio esperado no Proporcionado					
Errores Humanos / Falta de capacitación de Personal (interno y externo)	s	s	2	3	6
Falla en el Servicio de Telecomunicaciones	s	s	4	5	20
Falla en el Servicio de Energía Eléctrica	s	s	6	5	30
Evasión de Impuestos / Información tributaria errónea. Problemas con SRI	s	n	2	5	10
Daño de Instalaciones de Servicios básicos	s	n	2	5	10
Incumplimiento de Normas Ambientales	s	n	2	5	10
Riesgos por Desastres Naturales					
Incendios	s	n	4	7	28
Terremotos	n	n	4	7	28
Tormentas Eléctricas	s	n	2	5	10

* Hemos resaltado con rojo los riesgos de mayor impacto.

Al enfocarnos en los procesos del negocio y los riesgos del área de Sistemas, podemos anotar los siguientes:

ANÁLISIS DE RIESGOS ENFOCADO A PROCESOS		
Proceso	Riesgo asociado al negocio	Riesgo asociado a Área de Sistemas
Facturación	No existe la información de inventario disponible y a tiempo	No funciona la red
	La factura tiene errores	No funciona la base de datos
	El sistema falla y no se puede facturar	No existen respaldos de la información en caso de recuperación
		No se verifica el acceso no autorizado a las computadoras del personal
		No existe un plan de continuidad ante una interrupción
		No existen procedimientos para respaldos
		No existen procedimientos de recuperación

Producción	El sistema Élite falla	No existe control de personal no autorizado a la información de las fórmulas en el sistema
	La información de las fórmulas para fabricar los productos no es la correcta	No funciona la base de datos
	La información para la preparación de las fórmulas ha sido modificada	No funciona la red
	La información para la preparación de las fórmulas ha sido robada por algún empleado.	Existe personal no autorizado accediendo a los datos críticos del sistema
		No existen procedimientos de autenticación en la red de la organización

Abastecimiento	La información para distribución es incorrecta	No funciona la red
	La información para la distribución no está disponible	No existe un plan de continuidad del negocio ante una interrupción
	Incumplimiento de despacho a Clientes	No existen procedimientos para respaldos
	Incumplimiento de Materia Prima a empresas del grupo	Existen cartuchos no rotulados
		No existe control de los cartuchos de respaldo No existen procedimientos de recuperación Existe personal no autorizado accediendo a los datos críticos del sistema

Inventario	Pérdida de Control del Stock	No funciona la red
	Incorrecta Administración de Pedidos	No funciona la base de datos
		No se puede acceder al sistema oportunamente para emitir los pedidos
		No existen respaldos de la información

Crédito y Cobranzas	Falta de control en manejo de Cupo de clientes	No funciona la red
	Pérdida de recuperación de Cartera	No funciona la base de datos
	Incumplimiento de Obligaciones a Proveedores y Terceros	No existen respaldos de la información
		No se realizan oportunamente las actualizaciones de información en sistema alterno DOS.
		Existe personal no autorizado accediendo a los datos críticos del sistema

Una interrupción en el área de sistemas puede afectar considerablemente a la imagen de la empresa y ocasionar pérdidas irremediables si es en un largo tiempo.

Entre los riesgos más críticos para el área de Sistemas tenemos:

- Divulgación de información confidencial a terceros.
- Riesgo de pérdida parcial o total de información en caso de emergencia o desastre.
- Riesgos de integridad, disponibilidad y confidencialidad de información.
- Dificultad en la administración de la seguridad de información.

7.2.2 Análisis de los riesgos determinados para el Área de Sistemas

A continuación un análisis del impacto que tendrían sobre las operaciones del negocio estos riesgos y su probabilidad de ocurrencia.

Leyenda	Probabilidad	Impacto
Muy baja	2	1
Baja	4	3
Alta	6	5
Muy alta	8	7

Riesgo asociado a Área de Sistemas	Control	Ha Ocurrido	Probabilidad	Impacto	Severidad
No funciona la red	s	s	4	5	20
No funciona la base de datos	s	s	2	7	14
No existen respaldos de la información en caso de recuperación	s	n	2	7	14
No existen procedimientos para respaldos tanto de datos como de aplicaciones	s	n	2	7	14
No existe control de los cartuchos de respaldo	s	n	2	3	6
No existen procedimientos de recuperación	s	n	4	5	20
No se verifica el acceso de personal no autorizado al centro de cómputo	s	n	2	5	10
Existe personal no autorizado accediendo a los datos críticos del sistema	s	s	4	5	20
No existen procedimientos de autenticación en la red de la organización	s	n	2	5	10
No existe un plan de continuidad ante una interrupción	n	s	6	7	42
Que estén caducados los extintores cercanos al centro de cómputo	s	n	4	7	28
No funcionen los sensores de humo	s	n	2	7	14

* Hemos resaltado con rojo los riesgos de mayor impacto.

7.2.3 Conclusión

En base al análisis realizado, fueron detectadas varias oportunidades de mejora que sugerimos tomar en consideración con la finalidad de mitigar los riesgos relacionados con la administración, control y gestión de la infraestructura tecnológica de la Compañía así como también riesgos externos al área de Tecnología que producirían un impacto negativo en la operación de la empresa. A continuación nuestras observaciones y recomendaciones:

Procedimiento de Respaldo de Información.

Observación:

Los respaldos de información son generados en cintas magnéticas de 160/320 GB, las cintas que contienen información diaria son enviadas a un casillero en el Banco Bolivariano situado a pocas cuadras del edificio de Agripac, y además almacenadas dentro de las instalaciones del Departamento de Sistemas. Las cintas que contienen información semanal y mensual son almacenadas en una caja fuerte dentro de la oficina del Gerente de Sistemas. Así también se cuenta con respaldo semanal de las aplicaciones en el casillero del Banco. En caso de que se suscitara un desastre en horas no laborables del banco y que no se pudiera acceder al centro de cómputo, no se podría contar inmediatamente con las cintas. La empresa cuenta con un servidor alternativo de Replicación, pero éste se encuentra en un edificio contiguo a Agripac.

Actualmente no se guardan respaldos de la información de cada computadora de los usuarios.

Riesgo:

- No contar con las cintas inmediatamente en caso de emergencia o desastre.
- En caso de que sucediera un desastre en el área del edificio de la matriz, también se perdería la información del Servidor de Replicación.

Recomendación:

Se recomienda considerar los siguientes aspectos para mitigar el riesgo de pérdida total o parcial de la información respaldada en caso de emergencia o desastre:

- Realizar respaldos de toda la información crítica de la Compañía (documentos del personal, configuración de los sistemas operativos y herramientas utilizadas, mensajería, etc.)
- Se recomienda definir en el servidor de archivos, directorios personales para almacenamiento de información importante de los usuarios de la Compañía. De este modo, se simplificará el proceso de respaldo total de información al realizarse de manera centralizada en este equipo.
- Realizar pruebas frecuentes de restauración de información, con el propósito de corregir posibles errores en el proceso o incluir aspectos que no fueron contemplados con anterioridad, además de comprobar la integridad de la información respaldada.
- Mover el servidor de Replicación a un sitio lejano de tal manera que si ocurre un desastre en la Matriz, se pueda utilizar este servidor como respaldo.

Plan de Recuperación ante Desastre (DRP)**Observación:**

La compañía actualmente no cuenta con un plan de recuperación ante desastres (DRP) que considere los equipos y aplicativos que soportan los procesos críticos de la misma, el cual sería utilizado para mantener la continuidad de las operaciones en caso de una eventual destrucción/ daño temporal o permanente de las instalaciones o equipos que se encuentran ubicados en el centro de cómputo.

Existen algunos procedimientos de recuperación, pero no son suficientes para restaurar la operatividad completa del Centro de Cómputo.

Riesgos:

- En caso de emergencia, la falta de un plan de recuperación ante desastres (DRP) genera descontrol, incertidumbre y desorden. Por el contrario, si existiera y se mantuviera este documento actualizado, brindaría seguridad y sobre todo, establecería un control sobre cada uno de los componentes del sistema.
- Interrupción temporal o permanente de la continuidad de las operaciones de la compañía.
- Dificultad o imposibilidad de poder iniciar las operaciones en un centro de procesamiento alternativo, en caso de que el utilizado actualmente quede inhabilitado por alguna contingencia.

Recomendaciones:

La primera recomendación es elaborar un plan de recuperación ante desastres (DRP) que cubra a la compañía de los diferentes escenarios que pongan en peligro la integridad y la continuidad de las operaciones. El plan debe incluir los procedimientos para rehabilitar en el menor tiempo posible los procesos críticos del negocio, infraestructura informática, equipos y telecomunicaciones.

Comentarios de la Gerencia:

Para toda organización es altamente importante contar con un plan de recuperación de desastres, este no es solo un proceso de sistemas sino de toda la organización que además requiere de cierta inversión.

Como alternativa para cubrir una contingencia, la empresa cuenta con un servidor de respaldo en el edificio comercial de la matriz, el mismo que se actualiza en línea utilizando la herramienta de replicación de datos que maneja Informix.

Medidas de Seguridad Física en el Centro de Cómputo

Observación:

Se observaron ciertos detalles en el centro de cómputo que podrían ser mejorados y que se mencionan a continuación:

- Existencia de material combustible como papeles, alfombra en el Centro de Cómputo y salas contiguas
- No tienen instalado piso falso
- Existe un baño contiguo al Centro de Cómputo
- No existe un directorio telefónico cercano para llamar a Policía, Bomberos, etc.

Riesgos

- Eventual propagación de incendio, debido a la presencia de material combustible.
- Eventual daño de servidores y equipos de comunicación por inundación de baño contiguo.

Recomendación:

Se recomienda las siguientes actividades relacionadas a la seguridad física del Centro de Cómputo

- Se recomienda retirar el material combustible ubicado en el Centro de Cómputo, los materiales combustibles que deben mantenerse dentro del Centro de Cómputo deben ser mínimos, solo lo necesario.
- En los aparatos telefónicos deben colocarse los números de teléfono de emergencias, como las personas encargadas del Centro de Cómputo, proveedores, bomberos, etc.
- Instalación de piso falso en Centro de Cómputo.

Evaluación de la arquitectura de seguridad de información

Observación:

La compañía tiene instalado el Microsoft ISA Server como firewall para evitar la exposición a terceros de información confidencial y controlar los accesos externos no autorizados a la red LAN y WAN de la Compañía a través del enlace a Internet.

Se determinó que no se han realizado pruebas exhaustivas relacionadas a evaluar la confiabilidad del firewall respecto a la exposición a intrusos internos y externos como hackers, malos empleados y otros. Sólo se han hecho pruebas internas.

Riesgos inmersos:

- Exposición a terceros de información confidencial y estratégica de la compañía.
- Accesos no autorizados externos a la red local de la compañía.
- Pérdidas económicas debido al robo, pérdida o manipulación de información.

Recomendación:

Se recomienda considerar la necesidad de contratar con terceros la ejecución de un diagnóstico especializado y pruebas en los puertos de entrada / salida a Internet utilizado por la Compañía para probar la suficiencia del firewall adquirido, realizando mejoras y correcciones sobre las seguridades implantadas.

Seguridad de Instalaciones

Observación:

La compañía cuenta con guardianía las 24 horas del día, pero considerando que el Consulado de Inglaterra se encuentra en uno de los edificios de la matriz, al parecer no es suficiente en caso de atentados terroristas.

Riesgos inmersos:

- Exposición a posibles eventos terroristas.

Recomendación:

Se recomienda reforzar la seguridad del edificio, principalmente en horas de oficina.

8. ANÁLISIS DE IMPACTO DE NEGOCIOS

Agripac S.A. maneja diversos procesos en las diversas áreas funcionales del negocio, las cuales son las siguientes:

Recursos Humanos:

- Proceso de Selección
- Proceso de Reclutamiento
- Proceso de Capacitación
- Proceso de Nómina
 - Proceso de Roles
 - Proceso de Proveedores

Compras/Importaciones

- Proceso de Importación
- Proceso de Recepción
- Proceso de Costos/Liquidación
- Proceso de Proveedores Locales/Exterior
 - Proceso de Cotizaciones
 - Proceso de Ordenes de Compra
 - Proceso de Convenios

Finanzas

- Proceso de Cartera
 - Proceso de Control de Cupo de Clientes
 - Proceso de Aprobación de Solicitudes de Crédito
 - Proceso de Cobros directos / Puntos de Venta
 - Proceso de Manejo de Cheques Postfechados
- Proceso de Tesorería
 - Proceso de Bancos
 - Proceso de Cuentas por Pagar
 - Proceso de Emisión de Cheques
 - Proceso de Pagos Directos / Cobros-Depósitos
- Proceso Contable
- Proceso de Broker de Seguros
- Proceso Comercial
 - Proceso de Marketing
 - Proceso de Publicidad
 - Proceso de Promociones
 - Ventas
 - Proceso de Facturación
- Proceso de Operaciones
 - Proceso de Compras Locales
 - Proceso de Compras Exterior
 - Proceso de Producción
 - Proceso de Requerimiento/Recepción de Materia Prima
 - Proceso de Requerimiento de Producción
 - Proceso de Manejo de Maestros
 - Proceso de Ingreso de Producción
 - Proceso de Manejo de Lotes
 - Proceso de Manejo de envases/etiquetas/cajas
 - Proceso de Logística/Distribución/Abastecimiento
 - Proceso de Solicitud de Mercadería
 - Proceso de Emisión de Guías de Remisión
 - Proceso de Logística
- Proceso Técnico
 - Proceso de Charlas a Clientes
 - Proceso de Días de Campo
 - Proceso de Ensayos de nuevos productos

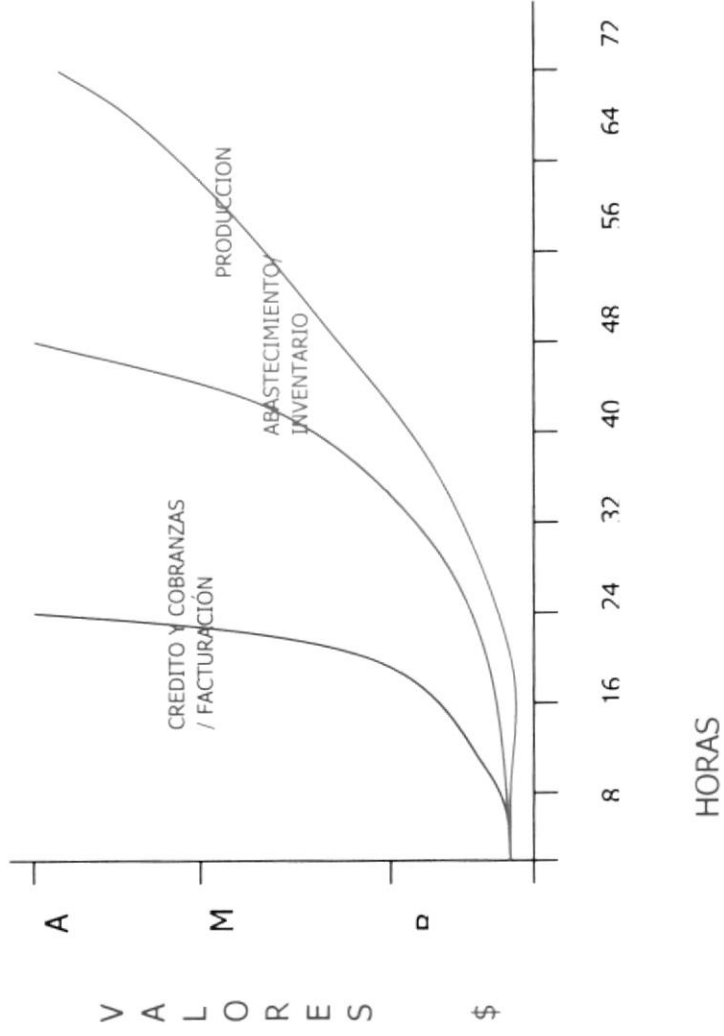
8.1 TABLA DE ANÁLISIS DE IMPACTO

EMPRESA	Agripac				
FUNCION	Importación, Fabricación y Comercialización de Insumos para la Agroindustria				
Procesos Básicos	Descripción del Impacto mas significativo	Rango de Pérdida	Sistema Requerido	Punto Crítico	Proceso Manual
Producción	Pérdida de Ventas por falta de Stock Pérdida de Imagen Corporativa	A	Elite	3 días	S
Facturación	Pérdida de Ventas - Mercado Cíclico Disminución del Mercado Pérdida de Imagen Corporativa	A	Elite/Aplicación DOS	1 día	S
Abastecimiento	Falta de abastecimiento a puntos de venta Disminución de Ventas Futuras Incumplimiento de despacho a Clientes Pérdida de Imagen Corporativa Incumplimiento de Materia Prima a empresas del Grupo	A	Elite/Aplicación DOS	2 días	N
Inventario	Pérdida de Control de Stock Incorrecta Administración de Pedidos	A	Elite/Aplicación DOS	2 días	S
Crédito y Cobranzas	Descontrol en Manejo de Cupo a Clientes Pérdida de recuperación de Cartera Incumplimiento de Obligaciones a Proveedores y Terceros	A	Elite/Aplicación DOS	1 día	S

A: Alto
B: Medio
C: Bajo
Prioridad de Recuperación: Elite

PUNTOS DE QUIEBRE

FACTURACIÓN	IT GENTE INFRAESTRUCTURA
PRODUCCIÓN	IT GENTE INSTALACIONES MAQUINARIA MATERIA PRIMA
CREDITO Y COBRANZAS	IT GENTE INFRAESTRUCTURA INSTITUCIONES CREDITICIAS
ABASTECIMIENTO	IT GENTE PRODUCTO TRANSPORTE
INVENTARIO	IT GENTE PRODUCTO INFRAESTRUCTURA



8.2 TABLA DE APLICACIONES CRÍTICAS

EMPRESA	Agripac			
FUNCION	Importación, Fabricación y Comercialización de Insumos para la Agroindustria			
Nombre de Aplicación	Proceso de Negocio que Soporta	Punto Crítico	Sistema Requerido	Incidencia
Elite	Producción	3	SCO Unix - Informix	A
	Facturación	1	SCO Unix - Informix	A
	Abastecimiento	2	SCO Unix - Informix	A
	Inventario	2	SCO Unix - Informix	A
	Crédito y Cobranzas	1	SCO Unix - Informix	A

8.3 CÁLCULO DEL TIEMPO DE RECUPERACIÓN

EMPRESA		Agripac					
FUNCION		Importación, Fabricación y Comercialización de Insumos para la Agroindustria					
Proceso	Tiempo Máximo de			Sincronización			Total
	Recuperación	SW Operacional	Aplicaciones	Act. De Datos	Manual		
Producción	72	6	4	8	4	22	
Facturación	24	6	4	8	6	24	
Abastecimiento	48	6	4	8	4	22	
Inventario	48	6	4	8	6	24	
Crédito y Cobranzas	24	6	4	6	6	22	

CÁLCULO DEL TIEMPO DE RECUPERACIÓN CON CENTRO ALTERNO

EMPRESA		Agripac					
FUNCION		Importación, Fabricación y Comercialización de Insumos para la Agroindustria					
Proceso	Tiempo Máximo de			Sincronización			Total
	Recuperación	SW Operacional	Aplicaciones	Act. De Datos	Manual		
Producción	72	0	0	0	4	4	
Facturación	24	0	0	0	6	6	
Abastecimiento	48	0	0	0	4	4	
Inventario	48	0	0	0	6	6	
Crédito y Cobranzas	24	0	0	0	6	6	

8.4 Conclusión

Agripac S.A. cuenta con un Sistema ERP que permite manejar de manera integrada los procesos operativos del Negocio, esto hace que de cierta forma sea manejable levantar las aplicaciones para dichos procesos a la vez en caso de presentarse una eventualidad. Para efectos de este análisis se ha establecido procesos críticos en base a su alta dependencia de IT. Por tanto dentro del Análisis de Impacto se han considerado los siguientes aspectos:

Debido a que Agripac S.A. es una organización líder en el mercado, que comercializa los productos elaborados por el grupo de empresas; y luego de realizar entrevistas con los dueños de procesos se ha podido identificar que sus operaciones son automatizadas y que cuentan a la vez con procedimientos manuales definidos en caso de prescindir de los automatizados.

Considerando que sus Ventas son cíclicas, en temporadas bajas serían usados y no afectaría en gran manera dentro de sus operaciones normales por un lapso de tiempo máximo de 3 días, pero si esto ocurriera dentro de las temporadas consideradas altas el riesgo operacional aumenta y se reduciría a 1 día ya que no es manejable a través de procesos manuales, ocasionando pérdida de oportunidades de Ventas que conllevan una disminución de mercado y por tanto pérdida de imagen Corporativa.

De igual forma la organización produce en gran parte los insumos que son comercializados, por ello cuentan dentro del sistema con un módulo de producción el cual ayuda a establecer los parámetros técnicos necesarios para obtener el nivel de calidad requerido dentro de cada producto elaborado, y el no contar con dichos parámetros no garantizaría el nivel del producto y no manejar adecuadamente los costos involucrados en el proceso, ocasionando pérdida de imagen corporativa y de ventas por falta de stock, por tanto el tiempo máximo de recuperación se estima en 3 días.

Agripac S.A. cuenta con una cantidad de Puntos de Venta considerables dentro de todo el territorio nacional (125 puntos de Venta) por tanto es crucial que el proceso de Abastecimiento que se realiza de manera semanal a los Sub-centros sea adecuado y oportuno para cumplir con los despachos a Clientes, aunque siempre manejan márgenes de stock dentro de cada punto de Venta que cubren para un mes por tanto el tiempo máximo de recuperación se estima en 2 días.

El número de ítems manejado por su diversidad de líneas de productos dentro del área agrícola hace difícil un proceso manual para el control de los mismos, por tanto se dificultaría la administración de pedidos el no contar con un sistema de inventario, por tanto se estima que el tiempo máximo de recuperación es de 2 días.

A su vez la organización posee una cartera de clientes considerable dentro de todo el territorio ecuatoriano y debido a que ellos cuentan con el servicio en diversas zonas del país se torna difícil el control de Cupos ya que no todos los puntos de Venta se encuentran en línea, por tanto se manejan controles manuales que ayudan a mitigar dicho riesgo pero se torna aun más difícil no contar con sistemas automatizados. Este descontrol a su vez haría incurrir en pérdida de recuperación de cartera lo que conlleva en incumplimientos de obligaciones con sus Proveedores y terceros, por tanto se estima que el tiempo máximo de recuperación es 1 día.

Nómina es uno de los procesos que se encuentra apoyado fuertemente con un sistema automatizado pero existen procesos manuales que reemplazarían fácilmente el manejo y control del mismo en caso de contingencia.

Con la existencia de un Centro Alterno que se maneje a través de Replicación estos tiempos determinantes para la normal operatividad de estos procesos dependientes altamente de tecnología estaría cubierto, el tiempo de activación del Centro Alterno es menor que el tiempo máximo de recuperación de dichos procesos además de la existencia de un Aplicación Alternativa denominada Aplicación DOS la cual se encuentra en todos los puntos de Venta, de esta manera ayudaría a manejar dichos procesos al operar en contingencias mayores y para ello se manejan procesos alternos y procesos manuales para su correcta activación.

9. CRITERIOS PARA LA DECLARACIÓN DE CONTINGENCIA Y ACTIVACIÓN DEL CENTRO ALTERNO

De acuerdo a la capacidad de respuesta que AGRIPAC S.A. dispone para atender situaciones que comprometan la continuidad de sus operaciones, se hace necesario establecer criterios que permitan identificar condiciones que califiquen para la declaración de contingencia y/o activación del centro alterno.

Las definiciones que a continuación se señalan, proveerán una guía de lineamientos, para la toma de decisiones y la diferenciación de cuando se debe activar el centro alterno y/o realizar la declaración de contingencia. La activación del centro alterno implica el operar en modo de emergencia y la declaración de contingencia conlleva a la activación del Plan.

Los siguientes criterios han sido establecidos de acuerdo a los procesos vitales del negocio, para identificar en que momento se debe tomar la decisión de realizar la declaración de contingencia y/o activar el centro alterno.

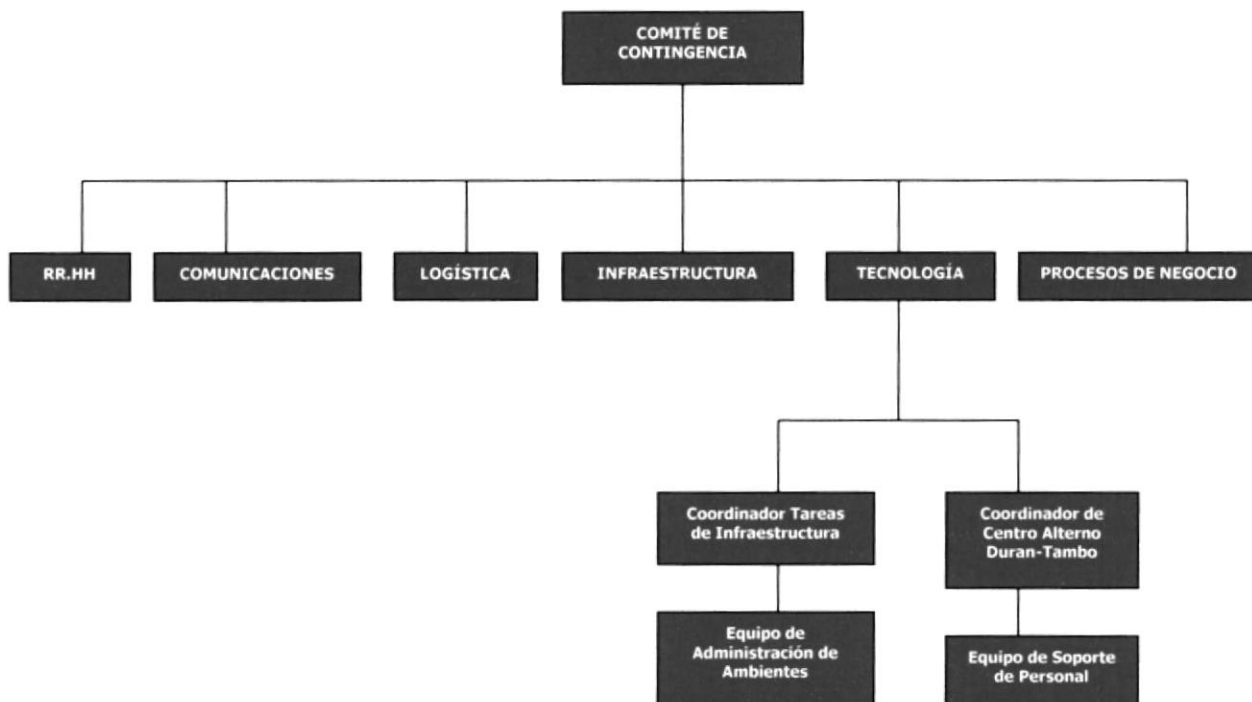
1. El Centro Alterno de Operaciones de AGRIPAC S.A. estará ubicado en el cuarto piso de las instalaciones de Balanfarina ubicada en el Km. 6 ½ de la vía Duran-Tambo.
2. El Centro de Operaciones para Ingreso de Datos estará ubicado en el segundo piso de la las instalaciones de Balanfarina.
3. El cliente interno dueño de los procesos críticos, identificados dentro del Análisis de Impacto determinó los servicios y recursos de interés en torno a los cuales se organizará el Plan y el dimensionamiento de recursos necesarios.
4. Se requerirá 8 horas a partir de la declaración de la contingencia habilitar las estaciones y montar las comunicaciones e infraestructura de red apropiada del Centro de Operaciones de Duran-Tambo (Centro Alterno), para que éste se encuentre completamente operativo.

9.1 FASES DEL PLAN DE ACCIÓN

1. Determinar la organización por contingencia.
2. Determinar el alcance de cada servicio durante la contingencia.
3. Determinar los escenarios de contingencia.
4. Identificar y priorizar los elementos críticos por servicio necesarios para operar durante la contingencia (recursos tecnológicos, de información, materiales, humanos, etc.).
5. Definir el modelo de operación de cada servicio durante la contingencia (grupos, responsabilidades, procedimientos, soportes, cronogramas, etc.).
6. Información y capacitación a los distintos grupos del modelo de operación.
7. Control y seguimiento durante la contingencia.
8. Plan de normalización de los servicios luego de la contingencia.

9.2 ESTRUCTURA ORGANIZATIVA PARA LA RECUPERACIÓN

El siguiente gráfico nos muestra como se deben organizar los equipos de trabajos para operar en modalidad de contingencia.



#	NOMBRE	CARGO CONTINGENCIA
1	Cristopher Bailey	Comité de Contingencia
2	Nicolás Armstrong	Comité de Contingencia
3	Bolívar Vallejo	Comité de Contingencia
4	Director Financiero	Comité de Contingencia
5	Jaime Bardavio	Coordinador de RR. HH.
6	Blanca Rodríguez	Asistente Coordinador de RR. HH.
7	Gisella Yépez	Equipo de RR. HH.
8	Lorena Hidalgo	Equipo de RR. HH.
9	Gustavo Wright	Coordinador de Procesos
10	Blanca Silva	Asistente Coordinador de Procesos
11	Gerónimo Alcívar	Equipo de Procesos
12	Miguel Jordán	Equipo de Procesos
13	Laura Delgado	Equipo de Procesos
14	Andrés Tacuri	Equipo de Procesos
15	Christopher Bailey	Coordinador de Comunicaciones
16	Elizabeth Sevilla	Asistente Coordinador de Comunicaciones
17	Ma. Mercedes	Equipo de Comunicaciones
18	Ma. Dolores Molina	Coordinador de Infraestructura/Evaluación de Daños
19	Segundo Méndez	Asistente Coordinador de Infraestructura/Evaluación de Daños
20	Marcos	Equipo de Infraestructura/Evaluación de Daños
21	Blanca Silva	Coordinador de Logística
22	Patricia Cucalón	Asistente Coordinador de Logística
23	Nelson Díaz	Equipo de Logística
24	Bolívar Vallejo	Coordinador de Tecnología
25	Hector Díaz	Coordinador de Centro Alterno
26	Manolo Viera	Coordinador de Infraestructura
27	Carlos Suárez	Equipo de Administración de Ambientes
28	Fernando Dela	Equipo de Administración de Ambientes
29	Jennifer Barrera	Equipo de Soporte a Personal
30	Wendy Rojas	Equipo de Soporte a Personal

10. EQUIPOS DE TRABAJO Y RESPONSABILIDADES

Esta sección identifica a los equipos de personas involucradas en el esfuerzo de recuperación y sus responsabilidades asociadas. Las actividades a desarrollar por estos Equipos de Recuperación de Operaciones han sido divididas en categorías antes, durante y después de una situación de Contingencia.

Las pautas consideradas para la conformación de estos equipos han sido las siguientes:

- Todo equipo debe estar conformado por un líder y un alterno.
- En cada equipo deben existir como mínimo dos participantes. El alterno puede ser uno de ellos.
- Ninguna persona debe estar participando en más de un equipo cuyas tareas, durante una Contingencia, sean concurrentes.
- Todas las personas identificadas en el Plan de recuperación de operaciones, deben conocer las responsabilidades que tiene que asumir.

Estas pautas se establecen con el fin de minimizar las posibilidades de no operatividad de los equipos debido a la ausencia de sus integrantes y/o al desconocimiento de sus responsabilidades.

En las próximas páginas se presentan los equipos, definidos en este Plan, con sus respectivos integrantes y en el anexo A se presenta la información relativa a los números telefónicos y direcciones de cada miembro de estos equipos.

10.1 Comité de Contingencia

Responsabilidades previas a una Contingencia

1. Compromiso de difusión de importancia del Plan de Contingencia y el papel de cada participante dentro del mismo.
2. Definir estrategias para proteger los activos de la institución, tanto humanos como materiales.
3. Autorizar políticas, procedimientos y controles para la protección y resguardo del patrimonio de la institución.

Responsabilidades durante la Contingencia

1. Autorizar ejecución de plan de respuesta o procedimientos para atender la emergencia.
2. Autorizar facilidades de recursos.
3. Evaluar los reportes de efectos o consecuencias reales y potenciales del incidente.

Responsabilidades después de la Contingencia

1. Evaluar los reportes de daños y autorizar operaciones de restauración.
2. Evaluar el desempeño de los procedimientos de atención de emergencias y evaluar tareas correctivas que ayuden a mejorar los planes de emergencias.
3. Evaluar la actualización de los planes de emergencias.

10.2 Equipo de RR. HH.

Responsabilidades previas a una Contingencia

1. Conocer y comprender el criterio de desastre del Plan de Operaciones en contingencia y normalización de servicios.
2. Conocer las tareas administrativas que se realizarán al momento en que ocurra una Contingencia.
3. Apoyar la realización de las diferentes pruebas de Contingencia.

Responsabilidades durante a una Contingencia

1. Solicitar al Equipo Gerencial la provisión de recursos que se utilizarán durante la operación en modalidad de Contingencia.
2. Organizar, ejecutar y controlar a primer nivel el cronograma de actividades de contingencia.
3. Coordinar la movilización hacia los hospitales o clínicas.
4. Proveer las facilidades al personal encargado de la recuperación.
5. Contratar al personal temporal (en caso de ser necesario).
6. Coordinar servicios médicos y alojamiento necesarios.

Responsabilidades después de la Contingencia

1. Evaluar el desempeño del sistema en modalidad de Contingencia.
2. Hacer recomendaciones al equipo gerencial para mejorar el Plan de Normalización de Servicios.

10.3 Equipo de Comunicaciones

Responsabilidades previas a una Contingencia

1. Coordinar el planeamiento previo de atención a emergencias con organismos públicos de seguridad.
2. Conocer y comprender el criterio de desastre del Plan de Operaciones en contingencia y normalización de servicios.
3. Conocer las tareas administrativas que se realizarán al momento en que ocurra una Contingencia.
4. Apoyar la realización de las diferentes pruebas de Contingencia.

Responsabilidades durante a una Contingencia

1. Solicitar al Equipo Gerencial la provisión de recursos que se utilizarán durante la operación en modalidad de Contingencia.
2. Organizar, ejecutar y controlar a primer nivel el cronograma de actividades de contingencia.
3. Contactar y coordinar con las compañías de seguros.
4. Contactar y coordinar el manejo de relaciones públicas y de proveedores.

Responsabilidades después de la Contingencia

1. Evaluar el desempeño del sistema en modalidad de Contingencia.
2. Hacer recomendaciones al equipo gerencial para mejorar el Plan de Normalización de Servicios.

10.4 Equipo de Logística

Responsabilidades previas a una Contingencia

1. Conocer y comprender el criterio de desastre del Plan de Operaciones en contingencia y normalización de servicios.
2. Conocer las tareas administrativas que se realizarán al momento en que ocurra una Contingencia.
3. Apoyar la realización de las diferentes pruebas de Contingencia.

Responsabilidades durante a una Contingencia

1. Solicitar al Equipo Gerencial la provisión de recursos que se utilizarán durante la operación en modalidad de Contingencia.
2. Organizar, ejecutar y controlar a primer nivel el cronograma de actividades de contingencia.
3. Contactar y coordinar con policía, departamento de bomberos y servicios médicos, las actividades a realizar.
4. Proveer transporte para equipos, personas y suministros.
5. Proveer dirección y número telefónico del Centro Alterno.
6. Coordinar pagos de facturas.

Responsabilidades después de la Contingencia

1. Evaluar el desempeño del sistema en modalidad de Contingencia.
2. Hacer recomendaciones al equipo gerencial para mejorar el Plan de Normalización de Servicios.

10.5 Equipo de Infraestructura

Responsabilidades previas a una Contingencia

1. Definir estrategias para proteger los activos de la institución, tanto humanos como materiales.
2. Organizar y entrenar grupos o brigadas de trabajadores para la atención de emergencias.
3. Conocer y comprender el criterio de desastre del Plan de Operaciones en contingencia y normalización de servicios.
4. Conocer las tareas administrativas que se realizarán al momento en que ocurra una Contingencia.
5. Apoyar la realización de las diferentes pruebas de Contingencia.

Responsabilidades durante a una Contingencia

1. Facilitar la evacuación de los ocupantes de las instalaciones, en caso de ser necesario
2. Evaluación inicial del estado de infraestructura de daños estructurales de las instalaciones físicas y de comunicaciones, número de evacuados y de heridos.
3. Reportar al Comité de Contingencia estado inicial de infraestructura de instalaciones físicas.
4. Tomar medidas de seguridad precautelares respecto de las instalaciones físicas.
5. Evaluar la magnitud de daño económico respecto de las instalaciones físicas y de comunicación.

Responsabilidades después de la Contingencia

1. Proteger las áreas afectadas.
2. Coordinar actividades de restauración de instalaciones físicas y de comunicación.
3. Evaluar el desempeño del sistema en modalidad de Contingencia.
4. Hacer recomendaciones al equipo gerencial para mejorar el Plan de Normalización de Servicios.

10.6 Equipo de Procesos

Responsabilidades previas a una Contingencia

1. Preparar y documentar los procedimientos manuales para la operación de los procesos críticos del negocio.
2. Establecer procedimientos de generación de información periódica (diaria, semanal, mensual, etc) de apoyo a procesos manuales de los procesos críticos.
3. Establecer los requerimientos mínimos de utilitarios y de los sistemas aplicativos para el desempeño de sus operaciones.
4. Conocer el plan de contingencia.
5. Asistir a las pruebas de contingencia.

Responsabilidades durante una Contingencia

1. Trasladar todos los recursos necesarios al site de seguridad.
2. Organizar, ejecutar y controlar a primer nivel el cronograma de actividades en contingencia.
3. Ejecutar procedimientos de operación de procesos críticos en modo de contingencia.

Responsabilidades después de la Contingencia

1. Evaluar el desempeño del modelo operacional de Contingencia de los procesos críticos.
2. Actualizar la documentación requerida del Plan de Normalización de Servicios.
3. Hacer recomendaciones al equipo gerencial para mejorar el Plan de Normalización de Servicios.

10.7 Coordinador de Tecnología

Responsabilidades previas a una Contingencia

1. Definir estrategias para proteger los activos de tecnología.
2. Formular políticas, procedimientos y controles para la protección y resguardo de equipos de tecnología.
3. Identificar y evaluar los riesgos que amenacen la continuidad operacional de la organización.
4. Elaborar y mantener planes de emergencia o de respuesta a incidentes.
5. Proveer soporte a otras dependencias de la organización en el desempeño de sus operaciones.

Responsabilidades durante la Contingencia

1. Ejecutar plan de recuperación de desastres para atender la emergencia.
2. Evaluar los efectos o consecuencias reales y potenciales del incidente y establecer los lineamientos de acción para mitigar los daños.
3. Reportar estado de situación de la emergencia al Comité de Contingencia.
4. Brindar apoyo logístico a los Equipos de trabajo de la contingencia y coordinar la administración de recursos para la reanudación de las operaciones.

Responsabilidades después de la Contingencia

1. Evaluar los daños y coordinar operaciones de restauración.
2. Evaluar el desempeño de los procedimientos de atención de emergencias y realizar las tareas correctivas que ayuden a mejorar los planes de emergencias.
3. Realizar la actualización de los planes de emergencias.

10.8 Equipo de Administración de Ambientes

Responsabilidades previas a una Contingencia

1. Prepara y Documentar los procedimientos de respaldo y recuperación del sistema operativo y programas producto.
2. Asegurar que los respaldos del sistema operativo y programas producto sean realizados periódicamente y enviados fuera de la instalación (bóveda).
3. Mantener actualizado en bóveda listados de configuraciones, inventario de equipos, etc.
4. Mantener actualizado en bóveda, el diagrama actual de conexiones de dispositivos de red.
5. Mantener en bóveda, reporte con las configuraciones actualizadas de los equipos de telecomunicaciones.
6. Mantener actualizado en bóveda, el listado de proveedores que puedan brindar apoyo.
7. Establecer los requerimientos del sistema operativo para los utilitarios, archivos y librerías indispensables para la operatividad de las aplicaciones críticas.
8. Verificar la funcionalidad entre las nuevas versiones del sistema operativo y las aplicaciones.
9. Actualizar la documentación técnica, a medida que se identifiquen cambios.
10. Asistir a las pruebas de contingencia.
11. Mantener actualizado el inventario de infraestructura requerida en el Centro Alterno.

Responsabilidades durante una Contingencia

1. Organizar, ejecutar y controlar a primer nivel el cronograma de actividades de contingencia.
2. Coordinar el reenrutamiento de la red de telecomunicaciones con las empresas proveedoras.
3. Ejecutar procedimientos de restauración del sistema operativo, y programas producto, en caso de ser necesario.
4. Poner en funcionalidad el sistema operativo, programas producto y las aplicaciones que se encuentran en el site de seguridad.

5. Ejecutar los pasos correspondientes para dar acceso temporal a los usuarios de las aplicaciones, en una máquina alterna.
6. Verificar la funcionalidad del sistema operativo y programas productos que se han activado en el site de seguridad.
7. Diagnosticar y solucionar problemas de telecomunicaciones que se vayan presentando. Documentar cambios realizados.

Responsabilidades después de una Contingencia

1. Evaluar el desempeño del sistema operativo en modalidad de Contingencia.
2. Actualizar la documentación requerida del Plan de Normalización de Servicios.
3. Hacer recomendaciones al equipo gerencial para mejorar el Plan de Normalización de Servicios.
4. Regresar equipos del Centro Alterno a ubicaciones originales.

10.9 Equipo de Soporte

Responsabilidades previas a una Contingencia

1. Preparar y documentar los procedimientos de provisión de soporte personalizado y mantenimiento correctivo de micros.
2. Dimensionar y preparar los materiales y recursos necesarios.
3. Respalda la información necesaria para la prestación del servicio.
4. Preparar y mantener soportes para procedimientos manuales referentes a su servicio.
5. Mantener el diagrama actual de conexiones de dispositivos de la red en el site de seguridad.
6. Mantener en bóveda, reporte con las configuraciones actualizadas de los equipos de telecomunicaciones.
7. Establecer los requerimientos del sistema operativo para los utilitarios, archivos y librerías indispensables para la operatividad de las aplicaciones críticas.
8. Conocer el plan de contingencia.
9. Asistir a las pruebas de contingencia.

Responsabilidades durante una Contingencia

1. Trasladar todos los recursos necesarios al site de seguridad.
2. Organizar, ejecutar y controlar a primer nivel el cronograma de actividades en contingencia.
3. Ejecutar procedimientos de prestación de servicios en contingencia.
4. Custodiar y mantener un inventario de activos puestos a su disposición.
5. Apoyar a los otros grupos de prestación de servicios en contingencia.
6. Documentar cambios realizados.

Responsabilidades después de la Contingencia

1. Evaluar el desempeño del modelo operacional de Contingencia referido a sus servicios.
2. Actualizar la documentación requerida del Plan de Normalización de Servicios.
3. Hacer recomendaciones al equipo gerencial para mejorar el Plan de Normalización de Servicios.

11. ESCENARIOS

Luego de la realización del *Análisis de Impacto de Negocio (BIA)* y el *Análisis de tiempo de recuperación*, se han identificado tres escenarios posibles, para los cuales Agripac S.A. debe definir procesos de preparación y prestación de servicios en modalidad de contingencia. Estos escenarios están en directa relación con la magnitud de la ocurrencia del evento y los efectos directos y posteriores que tal evento ocasionaría en la actual estructura de prestación de servicios.

Escenario	Motivo
1	Desastres naturales o provocados
2	Daños en los sistemas de información
3	Interrupción de servicios

Escenario #1

Desastres naturales o provocados

Concepto: Los **desastres naturales** son interrupciones que ocasionan que los recursos críticos de información queden inoperantes por un período que impacte adversamente las operaciones del negocio, como por ejemplo: terremotos, inundaciones (no aplicable para este plan), tornados, tormentas eléctricas severas, incendios, etc.
Los **desastres provocados** son eventos generados por seres humanos tales como ataques terroristas.

Escenario #2

Daños en los sistemas de información

Concepto: Existen servicios que no son catalogados como desastres, pero aún así tienen carácter de alto riesgo, por ejemplo: las interrupciones del servicio son causadas a veces por mal funcionamiento de los sistemas, eliminación accidental de archivos, corrupción de la base de datos, inconsistencias en el sistema operativo, daño o inconsistencia de las aplicaciones, ataques de negación de servicio, intrusos, virus.

Escenario #3

Interrupción del Servicio (Energía / Comunicaciones)

Concepto: Los eventos que causan interrupciones pueden ocurrir cuando los servicios esperados ya no son proporcionados a la compañía, como por ejemplo, el suministro de energía eléctrica, las **comunicaciones** u otros servicios entregados por externos (que pueden o no estar relacionados con un desastre natural).

Deben analizarse estrategias coherentes para cada escenario propuesto, sin embargo, para la realización de este plan solo se tomará en cuenta el **Escenario 1**.

Este escenario supone una destrucción parcial o total del Centro de Cómputo y sus activos, de tal manera que IT no podrá operar en el mismo sitio horas o días después de presentado el evento. Se involucran riesgos sobre la vida humana, motivo por el cual se hará referencia al *Plan de Respuesta a Crisis (Anexo)* ya definido para la institución, el que contempla todos los elementos indispensables para la evacuación, rescate y atención de personas afectadas por un desastre. Es por ello que el desarrollo de este Plan se enfocará en las actividades que IT deberá realizar para seguir prestando sus servicios en modalidad degradada (contingencia).

Para los escenarios 2 y 3 ya existen procedimientos de recuperación definidos, los cuales serán ejecutados de acuerdo al tipo de contingencia, éstos procedimientos se adjuntan como *anexos*. Cabe recalcar que en ambos escenarios el impacto de las amenazas identificadas no destruiría el Centro de Cómputo y tampoco habrá riesgo de pérdidas de vidas humanas.

12. ESTRATEGIAS DE RECUPERACIÓN

Desastres naturales o provocados

Una estrategia de recuperación es una combinación de medidas preventivas, detectivas y correctivas, que ayudan a:

- Eliminar la amenaza completamente.
- Minimizar la probabilidad que ocurra.
- Minimizar el efecto.

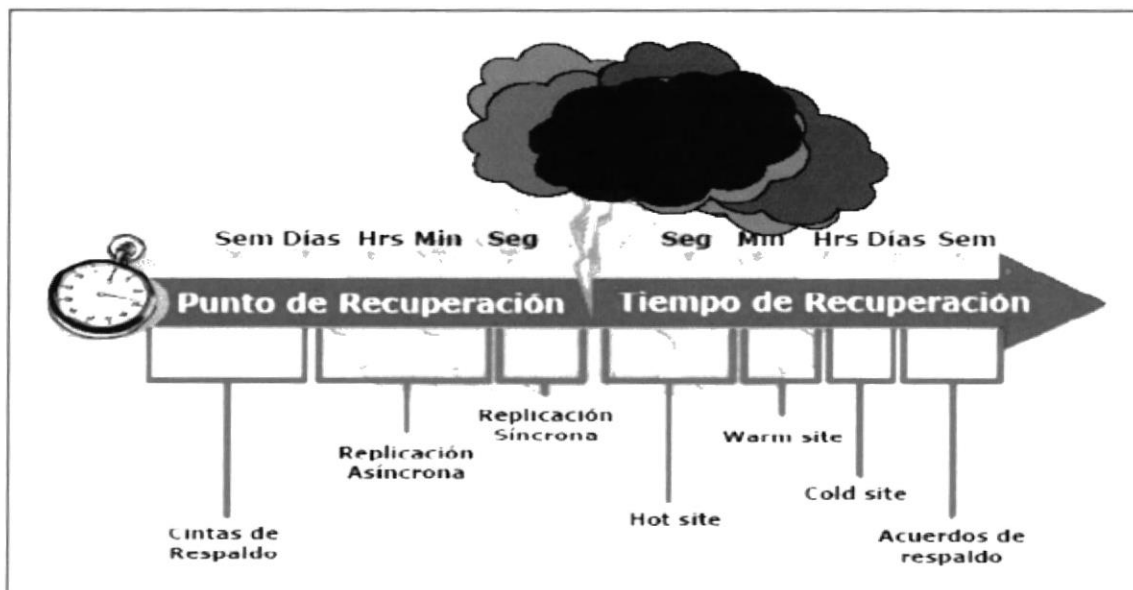
La estrategia apropiada es la que tiene un costo para un tiempo aceptable de recuperación que también es razonable con el impacto y la probabilidad de ocurrencia que se determinó en el *Análisis de Impacto de Negocio (BIA)*:

Proceso	Tiempo máximo de recuperación (horas)
Producción	72
Facturación	24
Abastecimiento	48
Inventario	48
Crédito / Cobranzas	24

En base a estos resultados se ha determinado que el tiempo en que IT debe recuperar sus operaciones es de **24 horas**, basándonos en el proceso de Créditos y Cobranzas, por tanto ahora pasamos a discutir cuáles son las alternativas de recuperación que **COBIT** menciona en su metodología.

12.1 Alternativas de recuperación

El siguiente gráfico ilustra como los tiempos de recuperación determinan la estrategia a seguir.



Estrategia	Detalle	Requerimientos adicionales
Hot Site	Configurados totalmente y listos para operar en varias horas.	Personal, Programas, Archivos de datos y documentación.
Warm Site	Parcialmente configurados y cuentan con: conexiones de red, discos duros, cintas y controladores.	Computador principal.
Cold Site	Ambiente básico: cableado eléctrico, aire acondicionado, piso, etc.; su activación puede tomar días o semanas.	Equipos, personal, programas, datos, documentación.
Acuerdos recíprocos	Entre organizaciones, promesa de procesamiento mutuo en caso de emergencia.	Configuraciones, nivel de compatibilidad entre partes del acuerdo.
Mirrored Site	Instalación espejo, alto tiempo de respuesta en emergencia, mayores costos.	Configuración baja o nula.

12.2 Situación actual

En la actualidad Agripac S.A. cuenta con un "Warm-Site" el cual se encuentra ubicado en un edificio contiguo (20 metros) del edificio principal, el cual incluye las siguientes características:

- Está equipado con una copia de la instalación del servidor principal **ELITE** : ERP y Base de Datos .
- Se ha definido el proceso de replicación en línea desde el servidor principal del **ERP ELITE** hacia el servidor alterno, a nivel de su base de datos **Informix**, explotando la fortaleza de **Informix** en cuanto a replicación se refiere.
- Las características de hardware del servidor alterno son similares al principal pero en un nivel degradado (menos memoria y disco).
- Se ha utilizado fibra para interconectar los sistemas entre los edificios principal y alterno.
- El edificio alterno brinda ciertas condiciones ambientales necesarias para la operación del servidor: UPS y Aire acondicionado.

A pesar de todos los puntos mencionados anteriormente, el centro de cómputo alterno no cuenta con las seguridades físicas necesarias tales como control de acceso físico, detectores de humo, extintor, control de entrada / salida. Adicionalmente no constituye una solución integral para las operaciones de todo el Centro de Cómputo, pues se encuentra en la misma área de impacto de un potencial desastre.

Por otro lado, las pruebas realizadas al Centro de Cómputo Alterno actual no han sido las adecuadas y se han restringido a subida de respaldos y ciertas pruebas de ingreso, lo cual no constituye ninguna garantía en el caso de una eventual desastre, dada la carga transaccional que podría tener el servidor alterno con el ingreso de un mayor número de usuarios.

12.3 ANÁLISIS DE IMPACTO FINANCIERO

Agripac S. A., depende en un alto grado de los servicios de información y tecnología IT, es un riesgo muy alto el que se corre al no contar con un centro de cómputo alternativo (que debe estar ubicado en otro sitio de la ciudad o fuera de ella), ya que de producirse un desastre natural o provocado que afecte la infraestructura de las instalaciones y/o paralice los servicios del actual centro de cómputo por más de tres días ocasionaría un enorme impacto que podrían paralizar de manera indefinida las operaciones de toda la organización.

Lo ideal es tener un centro alternativo FULL SITE, pero no se escogió esta opción porque demanda de una alta inversión, la opción seleccionada es un mix entre un WARM SITE y un HOT SITE, que permitirá contar en pocas horas con toda la información (base de datos completa) y todos los servicios pero en forma degradada dándole prioridad a los procesos críticos, de esta manera se podrá mantener las operaciones de todas las unidades del negocio hasta que se reestablezca un nuevo centro de cómputo.

La organización cuenta con un servidor de backup cuya configuración requiere ser actualizada con una baja inversión para que pueda operar como servidor de producción en caso de una contingencia, este servidor está conectado en línea al servidor de producción y se actualiza mediante un proceso de replicación que permite tener un espejo de la base de datos.

Para la implementación del Centro de Cómputo Alterno, hemos considerado aprovechar todos los recursos tecnológicos y de infraestructura que posee la organización para reducir los costo de inversión de este proyecto, es así que se escogió las instalaciones de Balanfarina para ubicar el centro de cómputo alternativo lo que incidirá significativamente en la reducción del costo de inversión, determinándose una inversión estimada de \$ 38.000 los que se distribuyen en los siguientes rubros:

Rubros	Costo	Porcentaje
Hardware	\$ 15.000	39.48 %
Software	\$ 5.000	13.15 %
Licencias	\$ 8.000	21.05 %
Mobiliario	\$ 10.000	26.32 %
Total	\$ 38.000	100.00 %

Esta cifra que resulta insignificante considerando que se está protegiendo y garantizando todas las operaciones de la organización, así como la continuidad y existencia misma del negocio en caso de un desastre natural o provocado.

TIPO DE SITE PARA CENTRO DE COMPUTO ALTERNO

Recursos	Requerimiento	Necesidades Cubiertas
Tipo de Site	Mix Warm Site -Hot Site	100 % degradadas
Hardware	Parcial	80 %
Telecomunicaciones	Parcial	70 %
Tiempo de Recuperación	Corto (36 horas)	70 %
Ubicación	Apropiada	90 %
Inversión o Costo	Bajo	

12.4 Selección y Desarrollo de Estrategia

En base a las secciones antes expuestas y luego de un análisis de:

- Tiempo de recuperación – resultado del BIA.
- Alternativas de recuperación – Metodología COBIT.
- Situación actual – IT (Agripac S.A.)
- Análisis Financiero

Adicionalmente, luego de la realización del análisis de riesgo, se hicieron recomendaciones para el Centro de Cómputo actual, la implementación de éstas ayudarán a mitigar ciertos riesgos encontrados, lo cual hará más coherente y efectiva la estrategia de recuperación seleccionada, ejemplo: la eliminación de material inflamable dentro del Centro de Cómputo mitigará el riesgo de que se propague un incendio.

Por todo esto se ha decidido que la mejor estrategia a desarrollar es un HOT SITE. La siguiente tabla ilustra las características que este site debe contemplar.

MIX WARM SITE - HOT SITE	
CARACTERÍSTICA	VALORACIÓN
COSTO	ALTO / MEDIO
HARDWARE	COMPLETO
TELECOMUNICACIONES	MEDIO
TIEMPO CONFIGURACIÓN	BAJO
UBICACIÓN	AJUSTADA

Para poder implementar esta alternativa de recuperación se llevarán a cabo las siguientes actividades, las mismas que completarán las características necesarias para que el MIX WARM SITE - HOT SITE pueda operar como se requiere.

Ubicación

La nueva ubicación del Centro de Cómputo Alterno será en una de las fábricas del Grupo, la cual cuenta con el espacio físico para albergar el Centro de Cómputo Alterno.

Nombre: **Balanfarina**

Ubicación: **Km 6½ de la vía Durán - Tambo**

El Edificio Administrativo de Balanfarina es de 4 pisos y se ha previsto instalar el Centro de Cómputo Alterno en su **Cuarto Piso**, bajo las mismas consideraciones de seguridad y ambientales ofrecidas por el Centro de Cómputo principal.

La disponibilidad y uso del resto de pisos del edificio, será dispuesto por el Comité de Contingencia de acuerdo a la evaluación de daños ocasionados por el desastre en las instalaciones principales de Agripac S.A. y el tiempo de recuperación necesario.

Este edificio estaría en capacidad de albergar a los usuarios de los procesos críticos, para que las operaciones del negocio continúen en modo degradado, por tanto, los funcionarios considerados en los equipos de contingencia y los no considerados deberán esperar instrucciones por parte del Comité de Contingencia. Sin embargo, este último tema no será cubierto por este plan, pues el objetivo definido es desarrollar las actividades para el funcionamiento de IT en contingencia.

Costo

La inversión necesaria será de \$ 38.000

Hardware

El hardware complementario citado en el Anexo B

Telecomunicaciones

Actualmente, la conexión entre los dos sites (Principal y Alterno), es del tipo L1 lo cual proporciona una velocidad de conexión 10 Mbps y el ancho de banda actual está siendo utilizado en un 50%.

Para el apoyo en la contingencia se instalará un anillo redundante de Comunicaciones, el cual operará inmediatamente el comité de contingencia declare la emergencia y lo comunique al proveedor para que se pueda hacer el cambio en el enlace.

Por último, cabe mencionar que existen *Acuerdos de Niveles de Servicio* definidos con el proveedor de Comunicaciones (Iseyko) los cuales garantizan los tiempos de respuesta mínimos requeridos desde el momento en que se declare la contingencia.

Tiempo de configuración

Este tiempo será bajo, pues la replicación es en línea y el cambio en la configuración se restringirá solamente a la parte de Comunicaciones.

Servicios Críticos

La definición de los servicios críticos se ha hecho en base a los procesos críticos identificados en el *Análisis de Impacto de Negocio (BIA)* que están soportados fuertemente por IT. Para ello debemos mencionar, en primera instancia, que todos los servicios que IT presta al Grupo Agripac y luego definir cuáles son los servicios que se activarán en contingencia y su alcance.

Los servicios que IT presta en condiciones de operación normal son los siguientes:

1. Mantenimiento de Hardware (Departamento Técnico).
2. Mantenimiento y Desarrollo de Aplicaciones.
3. Administración de Redes.
4. Administración de Base de Datos y Respaldos.
5. Mesa de Ayuda (Help Desk).
6. Instalaciones, movimientos y cambios.
7. Operaciones (Batch).
8. Adquisiciones.
9. Soporte Administrativo.
10. Control y seguimiento de activos (IT).

Como se mencionó anteriormente, éstos son todos los servicios que IT presta en operación normal, sin embargo cuando IT entra en Contingencia, no todos ellos pueden prestarse, más bien deben priorizarse en base a su criticidad y soporte a los procesos de negocio. Por ejemplo, el servicio de Mantenimiento y Desarrollo de Aplicaciones no prestará el elemento de servicio Desarrollo de Aplicaciones.

A continuación se detallan los servicios y los elementos de servicio que hemos definido como críticos y que van a prestarse durante la contingencia, dentro de cada uno de ellos establecemos cual es su alcance.

1. Mantenimiento de Hardware (Departamento Técnico).
2. Mantenimiento y Desarrollo de Aplicaciones.
3. Administración de Redes.
4. Administración de Base de Datos y Respaldos.
5. Mesa de Ayuda (Help Desk).
6. Operaciones (Batch).
7. Adquisiciones.
8. Soporte Administrativo.

* Los elementos de servicio que no apliquen serán identificados como N/A.

13. ESQUEMA DE PRESTACIÓN DE SERVICIOS EN CONTINGENCIA

Escenario: Desastres naturales o provocados

Servicio # 1

Nombre: Mantenimiento de Hardware

Descripción:

El área técnica funcionará en modo de contingencia, en la resolución de problemas de hardware que se presenten, dejando pendiente cualquier otra programación de tareas preventivas.

Elemento Servicio	Equipos	Materiales	Documentos	Responsable
Mantenimiento preventivo de HW	N/A	N/A	N/A	N/A
Mantenimiento correctivo de HW	Multímetro	Juego de desarmadores, cautín, diskettes de diagnóstico	Ficha de solicitud de servicio de sistemas	Carlos Suárez

Servicio # 2

Nombre: Mantenimiento y Desarrollo de Aplicaciones.

Descripción:

El servicio de Mantenimiento y Desarrollo de Aplicaciones, se orientará a garantizar en modalidad de contingencia la disponibilidad de la aplicación crítica:

- ERP Elite

Este servicio actuará como segundo nivel de resolución de problemas. *El procedimiento de prestación de servicios se apoyará en el esquema de petición directa de los Líderes de Procesos de Negocio y será validado por el Líder de Tecnología de otra forma no se prestará.*

El responsable del servicio prestará solo los servicios autorizados y registrará.

Elemento Servicio	Equipos	Materiales	Documentos	Responsable
Solicitud de cambios en programas	1 Computador	-	Procedimiento para solicitud de requerimientos de Software.	Héctor Díaz
Desarrollo proyectos	N/A	N/A	N/A	N/A
Adición o cambios en módulos (ERP e interfases)	N/A	N/A	N/A	N/A

Pruebas ambiente de pruebas	1 Computador	Servidor de pruebas	Procedimiento de ficha técnica de modificaciones	Héctor Díaz
Pruebas paso a producción	1 Computador	Servidor de pruebas	Procedimiento de pruebas de requerimientos y modificaciones	Héctor Díaz

Servicio # 3

Nombre: Administración de redes.

Descripción:

El servicio de administración de redes se orientará en modalidad de contingencia al mantenimiento de la disponibilidad de los servicios de red en el Centro de Cómputo Alterno. Este líder actuará como segundo nivel e solución de problemas y directos responsables de la operación, mantenimiento, resolución de problemas y custodia de los elementos de la red ubicados en el Centro de Cómputo Alterno. Sus acciones son proactivas y reactivas y apegadas a los procedimientos de operación en circunstancias normales.

Elemento Servicio	Equipos	Materiales	Documentos	Responsable
Instalaciones de red	-	Ponchadora, conectores, cuchilla, cable UTP Cat 5e	Ficha de solicitud de servicio de sistemas	Carlos Suárez
Solución de problemas	1 Computador	Teléfono	Ficha de solicitud de servicio de sistemas	Carlos Suárez / Fernando Dela
Monitoreo de red local	N/A	N/A	N/A	N/A
Monitoreo de enlaces	-	Proveedores contacto permanente	-	Carlos Suárez
Manejo de virus	Servidor de Antivirus	Consola	Procedimiento de manejo y control de virus	Carlos Suárez
Manejo de parches SO	N/A	N/A	N/A	N/A
Correo electrónico	Exchange	Consola	-	-
Internet	ISA Server	-	-	Carlos Suárez / Líder Tecnología

Servicio # 4

Nombre: Administración de Base de Datos y Respaldos.

Descripción:

Base de Datos

Se orientará a garantizar en modalidad de contingencia la disponibilidad de los datos, incluyendo la replicación, migración, archivo, manejo de espacio, respaldos y recuperación de datos, en las base de datos **Informix** que residan en los servidores de la red que han sido ubicados en el Centro de Cómputo Alterno. El responsable del servicio prestará sólo los servicios autorizados y registrará.

Esta prestación de servicios se apoyará en el esquema de petición directa de los líderes de procesos de negocio.

Respaldos

Mediante este proceso, el responsable firmará, registrará y recuperará los medios magnéticos almacenados en el casillero del Banco Bolivariano, conforme se requiera para las operaciones del Centro de Cómputo Alterno, registrando en la *Bitácora de Respaldos* los datos del medio magnético recuperado, así como los datos de quién recibe y demás datos relacionados.

Asimismo estará encargado de la realización de los respaldos diarios de acuerdo a las mismas políticas y procedimientos de respaldo definidos en operación normal.

Posteriormente en la fase de normalización de operaciones se registrarán los datos manuales de respaldo en el inventario electrónico definido para el efecto.

Elemento Servicio	Equipos	Materiales	Documentos	Responsable
Instalación de SO / Base de Datos			Procedimientos de configuración e instalación: - Unix - Informix	Fernando Dela
Definición y monitores de replicación	1 Computador	Escritorio	Procedimiento de replicación	Fernando Dela
Respaldo base de datos	Unidad Tape externa	Cintas 160/320 Gb	Procedimiento respaldo de base de datos Bitácora de respaldos sistema	Fernando Dela
Respaldos sistema operativo	Unidad Tape externa	Cintas 160/320 Gb	Procedimiento de respaldo de "file system" del sistema (Unix). Procedimiento de respaldo del sistema operativo (Windows).	Fernando Dela
Respaldo datos usuarios	N/A	N/A	N/A	N/A
Respaldo de programas fuente/objeto	Unidad Tape externa	Cintas 160/320 Gb	Llevados a BB	Alterno.

Servicio # 5

Nombre: Mesa de ayuda.

Descripción:

La Mesa de Ayuda (Help Desk), queda restringida a la modalidad de personalizado y priorizado en la resolución de problemas.

El procedimiento deberá realizarse a través de los Líderes de Procesos de Negocio de Agripac S.A. quienes piden el soporte al personal de la Mesa de Ayuda, luego de recibido el soporte técnico se llenará *la Ficha de solicitud de servicio de sistemas* el cual deberá ser firmada por el usuario.

Este servicio de soporte será sustituido por petición directa del Comité de Contingencia, por los servicios que actúen como segundo nivel en resolución de problemas.

Adicionalmente, la mesa de ayuda será el soporte directo para las **instalaciones, movimientos y cambios de computadores** a instalarse en el Centro de Computo Alterno, y sus funciones son:

- Instalación de equipos con Software base y aplicaciones.
- Puntos de red en directa sujeción a lo determinado por el responsable de Redes.
- Movimientos de equipos dentro del Centro de Cómputo Alterno.
- Adición del hardware y software declarado en el inventario de contingencia.

Para ello el Líder del Proceso de Negocio deberá indicar su necesidad de servicio a la Mesa de ayuda, firmará la Ficha de solicitud de servicios de sistemas, luego el técnico se movilizará con los materiales y los documentos necesarios para el registro de inventarios.

Elemento Servicio	Equipos	Materiales	Documentos	Responsable
Atención de problemas	1 Computador	Teléfono, Escritorio, Línea telefónica	Solo se atenderá a proceso críticos de negocio. Ficha de solicitud de servicio de sistemas	EQUIPO DE SOPORTE
Soporte telefónico	1 Computador	Teléfono, Escritorio, Línea telefónica	Registro en formato electrónico (Excel)	
Instalación de sistema operativo	-	Drivers, instaladores, parches.	Procedimiento de configuración e instalación de Windows	
Instalación de aplicaciones	-	Instaladores.	Procedimiento de configuración e instalación de Elite (Cliente)	
Movimiento de equipos	-	-	* Solo con aprobación de Líder de Proceso de Negocio	

Servicio # 6

Nombre: Operaciones (Batch).

Descripción:

El servicio de procesamiento del Centro de Cómputo en modalidad de contingencia se restringe a la ejecución de procesos Batch necesarios para la generación de Estadísticas, Consolidación de inventarios (desde puntos de Venta), Consolidación de Cartera, etc.; adicionalmente será responsable del proceso de impresión central (reportes): listado de clientes, listas de precios, etc., que se originen en el Centro de Operación Alterno y posterior a la impresión debe distribuirlos internamente.

Elemento Servicio	Equipos	Materiales	Documentos	Responsable
Procesos batch	-	-	Registro de procesos batch en formato electrónico (Excel)	Jennifer Barrera

Servicio # 7

Nombre: Adquisiciones.

Descripción:

Este servicio se encuentra descentralizado a Compras y no se prevee un gran número de requerimientos de adquisiciones, en todo caso si se presentarán se procederá de la siguiente forma:

Los Líderes de Proceso de Negocio solicitarán vía celular y/o teléfono convencional según aplique, al Líder de Tecnología el cual recogerá el pedido del usuario y lo registrará en su base de datos, procederá a pedir autorización al Comité de Contingencia quién aprobará o negará el pedido. En cualquiera de los dos casos el Líder de Tecnología comunicará al solicitante.

En caso de aprobación, el requerimiento se pasará al Soporte Administrativo, el cual buscare en la lista de proveedores definidos para la contingencia, se cotizará y se pasará luego al proceso de Compras.

Servicio # 8

Nombre: Soporte Administrativo.

Descripción:

Este servicio se encargará de mantener la documentación que se genere en el Centro Alterno y de proveer la documentación necesaria para la prestación de servicios en modalidad de contingencia.

Además este servicio se encargará del control y seguimiento de activos, deberá registrar todos los movimientos de inventarios que se produzcan durante la etapa

de contingencia en formatos manuales que quedarán bajo la custodia del dueño del servicio hasta que en la etapa de la normalización del servicio sean ingresados en la base de datos del inventario. Estos activos serán registrados bajo responsabilidad del usuario, quien se comprometerá por escrito por la integridad de los mismos y comunicará al dueño del servicio en caso de presentarse alguna eventualidad.

Elemento Servicio	Equipos	Materiales	Documentos	Responsable
Información de contactos	1 Computador	Mobiliario de oficina.	- Contratos - Proveedores	Wendy Rojas
	1 Impresora láser	Utilería: papel, reglas, carpetas, etc. ..	- Cotizaciones - Licencias - Pólizas - Contactos	

El responsable de este servicio también tendrá la siguiente información necesaria para la contingencia:

Requerimiento	Documento
Lista del personal, con prioridades.	Anexo A
Números de teléfono del personal: celular y convencional, direcciones.	Anexo A
Números de teléfono de proveedores de software y direcciones.	Anexo C
Números de teléfono, direcciones de proveedores de equipos, suministros y servicios.	Anexo C
Números de personas a contactar en Centro de Operaciones Alterno (Balanfarina).	Anexo A
Números de teléfono de agentes de la compañía de seguros.	Contacto: Seguros Sucre
Números de teléfono y contactos de proveedores contratados: Ej. Comunicaciones	Anexo C

14. ENFRENTANDO LA CONTINGENCIA

Plan "Primeros Pasos" para activar la Contingencia

Paso	Actividad
1.	Líder de Tecnología se entera del evento y comunica vía celular a responsable del Soporte Administrativo.
2.	Equipo de Comunicaciones informa a los Líderes de cada equipo (se inicia árbol de llamadas), se prioriza la reunión del Comité de Contingencia.
3.	Paralelamente el Líder de Tecnología comunica a los <i>Puntos de Venta (Sucursales y Sub-Centros)</i> que pasen a modo de Contingencia y que facturen con el sistema off-line Aplicación DOS.
4.	Comité de Contingencia se reúne y pide informe de daños a: a. Líder de Tecnología. b. Líder de Infraestructura. c. Líder de RRHH
5.	Comité de Contingencia decide declarar la contingencia en base a informe de daños.
6.	Equipo de Comunicaciones notifica al Centro de Cómputo Alterno (Balanfarina) y autoriza el ingreso del personal. Paralelamente Tecnología despliega al Equipo de Administración de Ambientes al Sitio Alterno.
7.	Líder de Tecnología solicita a Administrador de Red coordine con el proveedor de Comunicaciones (Iseyko) el "switch" hacia el enlace de respaldo (pruebas).
8.	Administrador de Red comunica a Líder de Tecnología y al responsable de Administración de Datos y Respaldos del cambio exitoso al enlace de respaldo.
9.	Administrador de Datos y Respaldos, revisa el funcionamiento del ELITE e Informix.
10.	Líder de IT solicita al Equipo de Comunicaciones notificar a las Agencias que vuelvan a trabajar con el ERP Elite.

15. PLAN DE ACTIVIDADES DURANTE LA CONTINGENCIA

Actividad	Responsable
Facilitar la evacuación de los ocupantes de las instalaciones, en caso de ser necesario y en coordinación con el líder del Plan de Respuesta a Crisis.	Equipo de Infraestructura y Comité del Plan de Respuesta a Crisis
Seguir la Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos (según Plan de Respuesta a Crisis). [Anexo de contactos]	Equipo de Comunicaciones, Comité de Crisis
Realizar reconocimiento de víctimas del desastre, en caso de ser necesario y en coordinación con el líder del Plan de Respuesta a Crisis.	Equipo de Recursos Humanos
En caso de haber heridos, coordinar la movilización hacia los hospitales o clínicas que constan en los cuadros médicos de los Seguros Médicos contratados por la empresa (Ecuasanitas, Salud, Panamerican Life). Esto incluye la gestión con los seguros médicos y pólizas de vida de cada empleado y alojamiento de ser necesario.	Equipo de Recursos Humanos
Poner a buen recaudo los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan)	Equipo de Infraestructura y Logística
Reportar estado de situación de la emergencia a la Alta Gerencia y al comité de la Contingencia.	Los equipos: RRHH, Comunicaciones, Infraestructura, Logística e IT
Dar la señal de Desastre para continuar con las actividades de puesta en funcionamiento del Sitio Alterno (Procedimiento de Activación del Sitio Alterno).	Comité de Contingencia
Evaluar y coordinar la adquisición de recursos para la reanudación de las operaciones durante la operación en modalidad de Contingencia en el sitio alternativo.	Comité de la Contingencia luego del reporte de los equipos a su cargo
Contratar al personal temporal (en caso de ser necesario) u otorgar responsabilidades diferentes a los colaboradores de la empresa en caso de ser necesario que reemplacen a algún miembro de los equipos de la contingencia.	Equipo de Recursos Humanos
Proveer transporte para equipos, personas y suministros.	Equipo de Logística
Coordinar pagos de facturas.	Equipo de Logística

* Los equipos deberán dar reportes de sus actividades al Comité de Contingencia, sobre el avance del Plan y las sub-actividades relacionadas **cada 3 horas**.

16. PLAN DE NORMALIZACIÓN DE SERVICIOS LUEGO DE LA CONTINGENCIA

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

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o del centro alterno, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución.

A continuación las actividades consideradas para la normalización luego de una contingencia:

Actividad	Responsable
<p>Evaluar condiciones del centro de cómputo Principal. Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, qué sistemas se están afectando, qué equipos han quedado no operativos, cuáles se pueden recuperar, y en cuánto tiempo, etc. Adicionalmente se deberá avanzar en las labores de preparación del Centro de Cómputo Alterno.</p>	Equipo de Infraestructura
<p>Priorización de actividades del Plan de Continuidad. Toda vez que el BCP es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución. Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignamiento temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.</p>	Comité de la Contingencia
<p>Proceso de Compras Poner órdenes de compra para reemplazo de equipos, órdenes de servicio y/o reparación, en la medida de que sea necesario.</p>	Líder de Tecnología
<p>Cobro de Pólizas de Seguros aplicables a los daños presentados durante la contingencia. En el evento de que ocurriera una contingencia, y ya que contamos con la totalidad de los activos de la empresa asegurados por Seguros Sucre, la primera opción para recuperar las operaciones normales es recurrir al cobro de las pólizas de seguro. Si bien es cierto, este dinero no será devuelto en un plazo inmediato, eventualmente servirá para la adquisición de toda la infraestructura necesaria para que el negocio pueda funcionar paulatinamente como antes. Es vital entonces que el plan contenga la información clave de los seguros de la organización.</p>	Equipo de Comunicación
Supervisar la instalación del hardware, líneas, teléfonos, muebles, etc.	Equipo de Logística
Validar si las acometidas eléctricas están en condiciones adecuadas de funcionamiento.	Equipo de Administración de Ambientes y Equipo de Infraestructura

Verificar las condiciones de seguridad física del centro de cómputo principal y autorizar el reingreso del personal.	Líder de Contingencia y Equipo de Infraestructura
Inspeccionar las condiciones de operatividad de los equipos de cómputo.	Equipo de Tecnología
Preparar todos los respaldos de sistema operativo, aplicaciones, bases de datos, datos, redes.	Equipo de Administración de Ambientes (TI) y Equipo de Procesos de Negocio
Iniciar la fase de recuperación de información desde los registros manuales de contingencia o en base a la información del servidor de Replicación.	Equipo de Administración de Ambientes (TI) y Equipo de Procesos de Negocio
Inspeccionar las condiciones de operatividad de las instalaciones del Edificio Principal. Si está apto para recibir al personal, autorizar su reingreso, si no, coordinar para que se trasladen a Balanfarina, donde podrían efectuar sus operaciones en caso de que la contingencia durara mucho tiempo.	Equipo de Infraestructura, Logística, Comité de la Contingencia.
Inicio de prestación de servicios en modalidad de prueba.	Todos
Comunicación del fin de la contingencia.	Comité de Contingencia
Mejoramiento continuo del Plan de normalización de los servicios luego de la Contingencia.	Todos

Pasos para la reactivación del servicio desde Centro de Cómputo Principal

Paso	Actividad
1.	Líder de Tecnología decreta la salida de línea del sistema desde el Site Alterno .
2.	Equipo de Comunicaciones ordena a Sucursales y Sub-centros, trabajar con el sistema off-line Aplicación DOS .
3.	Líder de Tecnología solicita a Administrador de Red coordine con el proveedor de Comunicaciones (Iseyko) el "switch" hacia el enlace de principal restaurado.
4.	Administrador de Red comunica a Líder de Tecnología y al responsable de Administración de Datos y Respaldos del cambio exitoso al enlace de principal.
5.	Responsable de Administración de Datos y Respaldos saca respaldos del sistema y se traslada con ellos a Site Principal.
6.	Responsable de Administración de Datos y Respaldos carga respaldos al sistema y hace pruebas preliminares.
7.	Administrador de red define y hace pruebas con la replicación entre Site Alterno y Site Principal (restaurado).
8.	Administrador de red verifica comunicaciones a través de enlace restaurado.
9.	Líder de tecnología coordina la entrada progresiva de usuarios al Sistema, si el avance es el esperado, decreta la operación desde Site Principal.
10.	Equipo de Comunicaciones comunica a los <i>Puntos de Venta (Sucursales y Sub-Centros)</i> que pasen a modo de Normal y que facturen con ERP Elite .

** Dado que la normalización es un evento conocido, sus tareas deben programarse para realizarse en un fin de semana.*

Evaluación de Resultados

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, qué tan bien se hicieron, qué tiempo tomaron, qué circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, cómo se comportaron los equipos de trabajo, etc.

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

Retroalimentación del Plan de Acción

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

El otro elemento es evaluar cuál hubiera sido el costo de no haber tenido la Institución el plan de contingencias llevado a cabo.

17. ADMINISTRACION Y MANTENIMIENTO DEL PLAN DE CONTINUIDAD (BCP) DEL NEGOCIO

El Plan de Continuidad de Negocios es un documento dinámico, que debe ser actualizado periódicamente para que se reflejen en él los cambios operativos relacionados con el manejo y control de la información, así como los cambios tecnológicos que surgen a través del tiempo y ocasionan variaciones dentro de las prioridades establecidas en los riesgos.

El Comité de Contingencia tiene la responsabilidad final sobre la difusión, mantenimiento y pruebas periódicas del Plan de Continuidad.

El Comité tiene la facultad de nombrar un administrador del Plan de Contingencia quien tendrá entre sus principales funciones el constante monitoreo de los procesos, documentar los cambios, coordinar las pruebas del Plan y evaluar los resultados, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los procesos que funcionan adecuadamente.

EL administrador del Plan de Contingencia debe informar constantemente al Comité de cualquier novedad y pondrá a consideración de éste las recomendaciones y sugerencias de cambios que se deban realizar en el Plan de Contingencia y será el Comité de Contingencia quien tome la decisión final de aprobar, modificar o rechazar las recomendaciones o cambios propuestos.

El Comité mantendrá constante comunicación con la Gerencia General para coordinar todas actividades referentes al Plan especialmente la difusión a los nuevos colaboradores, así como las pruebas y cambios significativos en el Plan de Contingencia.

ANEXOS

ANEXO A: DIRECTORIO DE MIEMBROS DEL EQUIPO DE RECUPERACIÓN

ANEXO B: RECURSOS MÍNIMOS DE RECUPERACIÓN

ANEXO C: DIRECTORIO DE PROVEEDORES

ANEXO D: DIAGRAMA Y CONFIGURACIÓN DE COMUNICACIONES

ANEXO E: PROCESOS ALTERNOS MANUALES

ANEXO F: PROCEDIMIENTOS

ANEXO A:

**DIRECTORIO DE MIEMBROS DEL EQUIPO DE
RECUPERACIÓN**

MIEMBROS DEL EQUIPO DE RECUPERACIÓN

#	NOMBRE	CARGO CONTINGENCIA	TEL.DOM.	CELULAR	DIRECCION
1	Christopher Bailey	Comité de Contingencia	2-870718	099-401721	CDLA. PUERTO AZUL MZ E9 VILLA 27
2	Nicolás Armstrong	Comité de Contingencia	2-835065	099-449621	CDLA LOS LAGOS AV. SEGUNDA Y AV. SUR
3	Bolívar Vallejo	Comité de Contingencia	2-834450	099-401557	URB. AQUAMARINA
4	Hakan Rindborg	Comité de Contingencia	2-560400	094-605947	CÓRDOVA 623 Y PADRE SOLANO
5	Jaime Bardavío	Coordinador de RR. HH.	2-885369	097-148367	5 LOMAS DE URDESA CALLE AVILÉS MZ M SOLAR 6 COND V-hermo-
6	Blanca Rodríguez	Asistente Coordinador de RR. HH.	2-236920	099-608836	SAMANES 6TA. ETAPA MZ 950 SOLAR 20
7	Gisella Yépez	Equipo de RR. HH.	-	097-832610	HUANCAVILCA CIUDAD DEL NORTE MZ I VILLA 23
8	Lorena Hidalgo	Equipo de RR. HH.	2-236256	099-303514	HUANCAVILCA CIUDAD DEL NORTE MZ M VILLA 63
9	Gustavo Wray	Coordinador de Procesos	2-831531	094-606923	CONJUNTO SANTA LUCÍA KM. 2.5 VÍA SAMBORONDÓN
10	Blanca Silva	Asistente Coordinador de Procesos	2-852261	099-406846	CEIBOS NORTE CALLE PRIMERA No.303
11	Gerónimo Alcivar	Equipo de Procesos	2-250524	099-425329	URB. SAN FELIPE MZ 129 VILLA 3
12	Miguel Jordán	Equipo de Procesos	2-811012	097-502085	CDLA. BRISAS DE SANTAY MZ F VILLA 17 A
13	Laura Delgado	Equipo de Procesos	2-252198	099-426368	MARTHA DE ROLDÓS MZ 707 VILLA 21
14	Andrés Tacuri	Equipo de Procesos	2-213495	099-426450	SAMANES 5 MZ 936 VILLA 23
15	Christopher Bailey	Coordinador de Comunicaciones	2-870718	099-401721	CDLA. PUERTO AZUL MZ E9 VILLA 27
16	Elizabeth Sevilla	Asistente Coordinador de Comunicaciones	2-244598	099-484538	CDLA. ALBORADA 4TA. ETAPA MZ EG VILLA 5
17	Ma. Mercedes Cortéz	Equipo de Comunicaciones	2-448255	097-386297	JOSÉ VICENTE TRUJILLO 115 Y JOSÉ SALCEDO
18		Coordinador de Infraestructura/Evaluación de Daños			
19	Ma. Dolores Molina	Asistente Coordinador de Infraestructura/Evaluación de Daños	2-851082	099-421050	CEIBOS NORTE, LA CUMBRE MZ 5 C SOLAR 12
	Segundo Méndez		2-248350	099-608839	ALBORADA 11 AVA. ETAPA MZ 36 VILLA 2

20	Marcos Pérez	Equipo de Infraestructura/Evaluación de Daños			097-448205	FLORIDA NORTE MZ 373 SOLAR 3
21	Bianca Silva	Coordinador de Logística	2-852261	099-406846	CEIBOS NORTE CALLE PRIMERA No.303	
22	Patricia Cucalón	Asistente Coordinador de Logística	2-412311	094-501954	PINOROCA 409 Y CHILE	
23	Nelson Díaz	Equipo de Logística	2-423780 - 422816	094-135783	FLORESTA 3 MZ T VILLA 2	
24	Bolívar Vallejo	Coordinador de Tecnología	2-834450	099-401557	URB. AQUAMARINA	
25	Hector Díaz	Coordinador de Centro Alterno	2-801694	099-422274	CIUDAD ABEL GILBERT MZ A 38 VILLA 6	
26	Manolo Viera	Coordinador de Infraestructura	2-866434	099-402711	CDLA. PEDRO MENENDEZ MZ 1 SOLAR 15	
27	Carlos Suárez	Equipo de Administración de Ambientes	2-252198	099-407787	MARTHA DE ROLDÓS MZ 707 VILLA 21	
28	Fernando Dela	Equipo de Administración de Ambientes	2-255500	091-960909	URB. SAN FELIPE MZ 127 VILLA 19	
29	Jennifer Barrera	Equipo de Soporte a Personal	2-820288	093-775006	GUAYACANES MZ 86 VILLA 11	
30	Wendy Rojas	Equipo de Soporte a Personal	2-386740	097-468865	CDLA. URDESA CENTRAL, LAS AGUAS 1205 Y LAURELES	

ANEXO B:

RECURSOS MÍNIMOS DE RECUPERACIÓN

RECURSOS MÍNIMOS DE RECUPERACIÓN

Una vez identificados los procesos críticos que permitirán garantizar la continuidad del negocio los que están incorporados como parte de este Plan de Continuidad del Negocio (BCP), es importante establecer los recursos humanos y materiales (mobiliario, hardware, software) mínimos requeridos para el funcionamiento del sitio alternativo, los que detallamos a continuación.

Equipo de Recursos Humanos para Operar el Centro de Cómputo Alterno

CARGO	NOMBRE	FUNCIÓN
Líder de Sistemas	Bolívar Vallejo	Responsable del correcto funcionamiento del centro de cómputo alternativo, de la integridad, confiabilidad y seguridad de los datos, encargado de coordinar las actividades con los miembros de los otros equipos durante la emergencia
Encargado de Redes	Carlos Suárez	Responsable del correcto funcionamiento de red LAN y de las redes WAN
Especialista en Base de Datos	Fernando Dela	Encargado de controlar que la base de datos del servidor de replicación funcione adecuadamente y se mantenga actualizada
Responsable del ambiente de Producción	Héctor Díaz	Debe garantizar que todos los aplicativos en especial los procesos críticos estén disponible, funcionen manteniendo las seguridades y controles en cada uno de los procesos
Responsable de Comunicaciones	Manolo Viera	Coordinar con los proveedores de comunicación y garantizar el correcto funcionamiento de las comunicaciones entre el centro de cómputo alternativo y las plantas y puntos de ventas
Operador de los procesos Batch	Jennifer Barrera	Responsable de procesar todas las transacciones que se reciben de los puntos de ventas que trabajan fuera de línea, en las aplicación centralizada elite

Inventario de Activos del Centro de Computo Alterno

EQUIPO	CARACTERISTICAS	IDENTIFICACION
1 Servidor Compaq Proliant 8000	2 Procesadores Zeon 2.GHz, 1 GB RAM Arreglo de Discos RAID V Tarjeta de Comunicaciones Equinox Mega Port 16 P. Tarjeta de Red, CD, Floppy, Puerto Serial	AGH-001
1 Unidad de Cinta DLT	160-320 Gyga Bytes	AGH-002
1 Servidor Intel 4508 (Mensajería)	2 Procesadores Zeon 3.0 GHz, 2 GB RA, Arreglo de Disco RAID I, Tarjeta de Red, CD-R, Puerto Serial	AGH-003
1 UPS Marca Best Power	3 KVA	AGH-004
2 Switch Marca CISCO	24 Puertos de 100 Mega Bits	AGH-005
4 Routers	CISCO de 2 Puertos	AGH-006
10 PC Genéricos	Pentium IV de 3.2 Mhz 256 RAM, HD 80 GB, CD Tarjeta de Red, Puertos Serial, USB, Monitos 15 ", Teclado, Mouse	AGH-007
3 Impresoras	Laser de 18 ppm	AGH-008
5 Modem Motorola	56,2 bps	AGH-009
10 Líneas de Telefono	Digitales de Pacifictel	AGH-010
1 Copiadora	Xérox	AGH-011
1 Fax	Panasonic	AGH-012

Inventario de Software del Centro de Cómputo Alterno

SOFTWARE	CARACTERISTICAS	IDENTIFICACION
1 Licencia de SCO UNIX Open Server	Versión 5.25	AGS-001
5 Licencia de SCO UNIX, Usuarios	Versión 5.25	AGS-002
1 Licencia Informix DBA Server	Versión 7.23	AGS-003
5 Licencias de Informix 4GL Runtime	Versión 7.23	AGS-004
Software aplicativo integrado Elite	Versión 6.0.2 R	AGS-005
Windows Server 2003	Versión 2003	AGS-006
Exchange Server	Versión 2003	AGS-007
Isa Server 2003	Versión 2003	AGS-008
10 Licencias Antivirus Mail Scan Server	Mail Scan	AGS-009
10 licencias Antivirus F-Prot Professional	F-PROT para estaciones	AGS-010
10 Licencias Windows XP	Windows XP	AGS-011

Inventario de Mobiliario requerido para el funcionamiento de los Procesos Críticos durante la activación del Plan de Contingencia

DESCRIPCION	CODIGO	DISPONIBILIDAD
1 Vehículo pequeño	AG001	SI
1 Vehículo transporte personal	AG002	SI
5 Teléfonos convencionales	AG003	NO
4 Celulares	AG004	NO
2 Radios de Comunicaciones con frecuencia interprovincial	AG005	NO
10 Escritorios	AG006	NO
10 Sillas	AG007	NO
3 Calculadoras	AG008	NO
2 Perforadoras	AG008	NO
3 Engrapadoras	AG009	NO
1 Saca Grapas	AG010	NO
4 Cajas de Clips	AG011	NO
4 Block de notas	AG012	NO
100 hojas de papel Bond A4	AG013	NO
5 Plumas	AG014	NO
5 Lápices	AG015	NO

ANEXO C:

DIRECTORIO DE PROVEEDORES

DIRECTORIO PROVEEDORES

PROVEEDORES DE SERVICIO

NOMBRE	CONTACTO	TELEFONO	FAX	CELULAR	DIRECCION	PRODUCTO / SERVICIO	e-mail
Iseyco C.A.	Guillermo Vacas	2-289312 / 2-399157	2-286436	099-944398	1ero. de Mayo 1006 y Carchi Edif. Consorcio 3er piso	Servicio de enlace de comunicación con Balanf.	gvacas@gye.iseyco.com
Megadatos - Accesram	Katty Murillo / Silvia R.	2-687610 / 2-687600	2-687555 Ext.285	098-372835 / 098-020212	Norte- torre B 4to. Piso ofi.403	Servicio de Internet y enlaces	kmurillo@megadatos.net / srodriguez@megadatos.net
Sersitel S.A.	Víctor González	2-872767 / 2-872369	2-872369	099-671798	Urbanización Renacer Mz 138 Villa 2	Mantenimiento de redes telefónicas y centrales	
Conecel S.A. (Porta)	Ross Mery Cornejo. / Irlanda Lainez	2-693693	2-693684	099-422878 / 099-423594	Av. Fco de Orellana y Alberto Borges	Sevicio de Telefonía Celular	rcornejo@conecel.com
Edecatsi S.A	Fernando Dela	2-255500	2-255500		Cdla. San Felipe Mz. 127 # 19	Servicio y mantenimiento en el servidor, etc	edecatsi@hotmail.com
Fleet Call	Ma. Fernando Pillajo	2-682550	2-680881		Av. Fco. Orellana Mz 112 Solar 2A Edif. Telerama	Servicio de Radios en Pascuales y Guardias	mafer@trunkservice.net
Leo Sánchez Naranjo	Leo Sánchez	2-360193		099-643937	Sucre 707 y Guerrero Martínez	Mantenimiento y Reparación de equipos	lsanchez2766@hotmail.com
Metro Comunicaciones S.A.	Carmen Tapia	2-321717	2-329226		Córdova y 9 de Octubre Ed. San Fco. 300 Piso 25	Servicio de mensajería por metro	
Sermatec	César Ladinez	2-334998 / 2-445368		099-053580	Nicolás Augusto González 1817 y Los Ríos	Servicio y matenimiento técnico de copadoras	cladinez@telconet.net
Smart Solutions	Giovana Minchal / Spencer Velasteguí	2-645563 / 645532	2-645563	099-743126 / 099-269492	Cdla. La Garzota Mz 95 Solar 12	Servicios internet y enlaces	gminchala@smartsolutions.com.ec
Sismode Cia. Ltda.	Belinda De Filippi / Diego Arias	2-294417 / 2-286957	2-283509	099-524816 / 099-528499	Cdla. Albatros Miguel H. Alcivar y Plaza Dañín	Renta de equipos para control y despacho de bodegas	bdefilippi@sismode.com
Sys@dmin com. S.A.	Carlos Cruz	2-515519	2-305900	099-945453	Vélez 409 y Escobedo 1er Piso	Reordenamiento de líneas de ingreso a la Central	
Telesis S.A.	Ing. Víctor Salguero	2-306911 / 2-567201	2-308557		L. De Garaicoa 732 y V.M. Rendón 3er Piso of. 31	Servicios para la Central telefónica	
Xerox del Ecuador S.A.	Edmundo Merizalde A.	2-693440 / 2-693450	2-693460	094-251075	Edif. Centrum piso 14 ofic. 4- Av. Fco. De Orellana Al. Bor.	Servicio de copias	edmundo.merizalde@ec.xaco.xerox.com

PROVEEDORES DE EQUIPOS / PARTES / PIEZAS

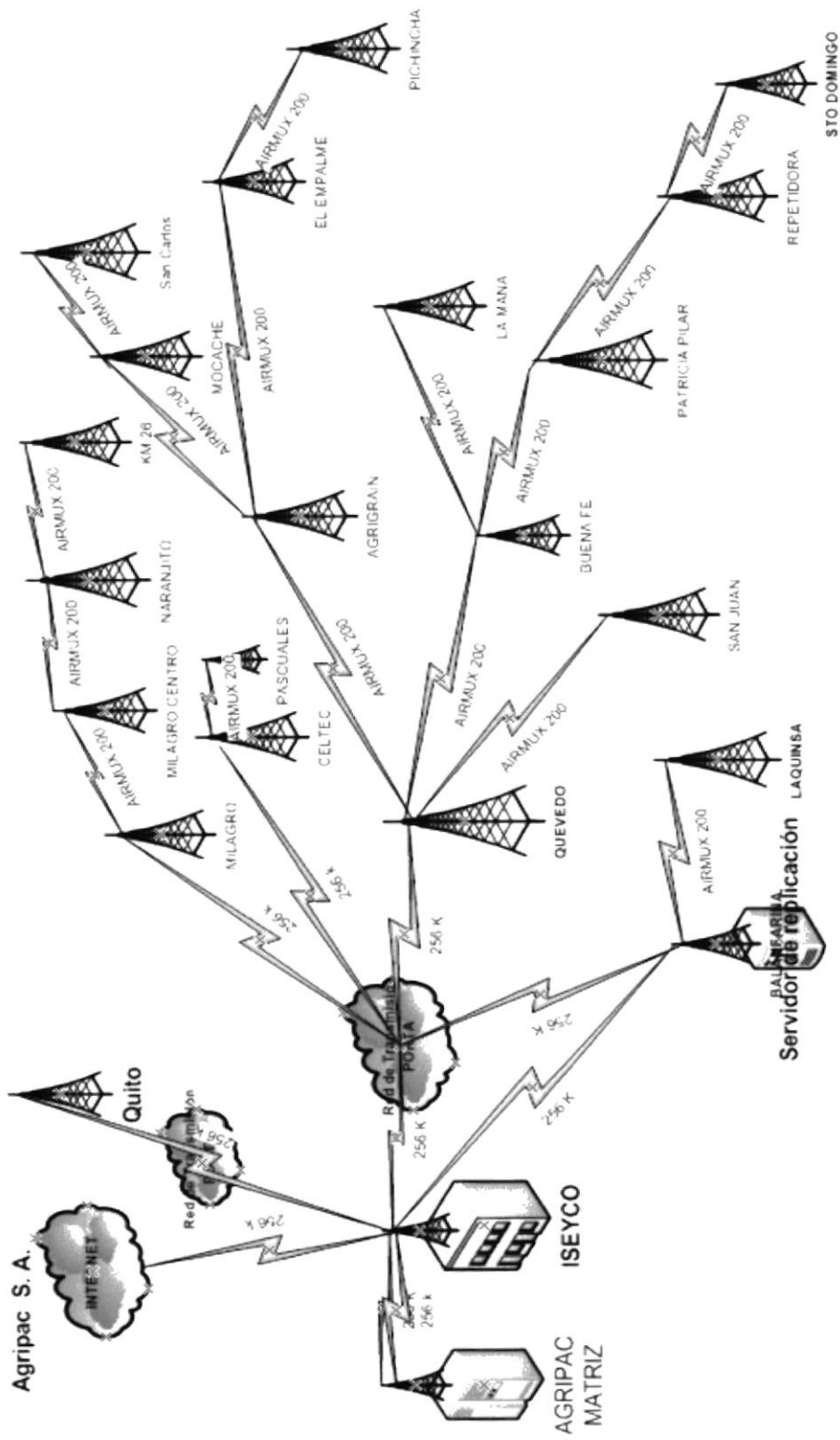
NOMBRE	CONTACTO	TELEFONO	FAX	CELULAR	DIRECCION	PRODUCTO / SERVICIO	e-mail
Akros Cia. Ltda.	Mariela Bajaña	2-386256 Ext.103	2-389666 Ext.131	099-297072	Víctor E. Estrada 104 entre Bálsamos y Circunvalación Norte Cdma. Albatros Calle Pelicano Oest. Mz V2 Solar 7 y Av. C.L	Computadoras, equipos de protección y accesorios	mariela.bajana@akroscorp.com
Alcatel - Telalca	Alba Apolo	2-281442	2-282011 2-642600 Ext. 20	093-148811	Cdma. La Garzota III, 4To. Pasaje VIII y Juan J. B	Venta de centrales telefónicas	alba.apolo@telalca.com
Celco Cia. Ltda.	Mónica Espinoza	2-642600				Baterías para Central telefónica, Aps y Ups	monica.espinoza@celco.com.ec
Compumillennium S.A.	Lcda. Jenny Jara / Paola López	2-522426 / 2- 325933	2-522426 Ext.110	094-137175	9 de Octubre 411 y Chile Edif. VALCO 3er. Piso C.C. Unicentro 2 Piso Local 203	Computadoras, equipos de protección y accesorios	jenny@compumillennium.com / paola.lopez@compumillennium.com
Compusariato C. Ltda.	Clara Rodríguez		2-324484	099-633136		Computadoras y accesorios	clararodriguezsilva@yahoo.com
Derten S.A.	Ing. Jaime Anchundia	2-320561 / 2- 325669	2-325669		Vélez 423 y Boyacá 4to. Piso -Of.10	Computadoras y accesorios	derthen2003@hotmail.com
Durapower	Ingrid Zuloaga	2-399051 / 2- 281548	2-398955	099-528742	Cdma. Guayaquil Mz 14 Villa 4	Baterías para Ups y Accesorios de computadoras	dpowegy@ecua.net.ec
E-Technology S.A.	Sandra Díaz / Ing. Luis Quiña	2-610947 / 2- 382744 / 2- 389424	2-610947	097-572020 / 097-571906	Urdenor II, Jaime R. A. 239- Av. J. T. Mar. 3piso Ed. Grafehi C.C. Primavera piso 2 ofic. 214 /Chimb. 2108 y Fco. de Marzo	Servicio de capacitación al personal, venta de equipos y de software	lquina@e-technology.com.ec
GBC Tech S.A.	Guido Becerra	2-402782 / 2- 404528	2-404528	096-021483		Discos, tarjetas para servidores	gbc_tech@yahoo.com
Indusur S.A.	Christian Camposano	2-201177 / 2- 200188	2-207249	099-345731	Av. C Julio Arosemena Km 4 vía a Daule	Venta / teléfonos y centrales telefónicas, consola	ventas.panasonic@indusur.com
Juan Marcet Cia. Ltda.	Victor Pineda	2-322990 / 2- 324444	2-321552		Pedro Carbo 1015 y Colón Kndy Norte Mz 308 Villa 6 Atrás del Edif. Centrum	Suministros de oficina / Acces. Computadoras	
Microsolutions S.A.	Yadira Meza	2-682482	2-682482	099-870994		Soluciones de redes- Sistemas-Aplicaciones Equipos y Accesorios para radios	ymeza@microsolutions-sa.com
Multicom S.A.	Vanessa Triviño / Rocío Castillo	2-208300 Ext.104/107	2-208308	097-482005 / 097-482293	Av. Carlos J. Arosemena 402 y Av. Miraflores esq.	Troncalizados	ventas@multicom.com.ec mespinoza_powersys@hotmail.com
Powersys S.A.	Miriam Espinoza	2-646047	2-646067	098-803437	Garzocentro 2000 Local 514	Baterías para Aps	
PPC	Maryuri valdiviezo / Guillermo Sánchez	2-381023 / 381523	2-381523	099425711 / 094038913	Costanera 812 entre Guayacanes e Higueras Av. Fco./ Orellana, Ed. World Trade C.-Torre A piso 8 of.802	Antivirus, softwares, hardwares, suministros	ventas@ppc-sa.com
Servapsa S.A.	Eco. Roxana Miranda	2-630177	2-630182	099-759497		Accesorios para radios Troncalizados	servapsa@andinanet.net
Service 21	Fabrizio Di Carlo	2-291912	2-291912 Ext.24	098818129	Av Las Americas Edif Sonapal planta alta	Accesorios y equipos para computadoras	fcarlo@service-21.net
Sismode Cia. Ltda.	Belinda De Filippi / Diego Arias	2-294417 / 2- 286957	2-283509	099-524816 / 099-528499	Cdma. Albatros Miguel H. Alcivar y Plaza Dañin	Renta de equipos para control y despacho de bodegas	bdefilippi@sismode.com

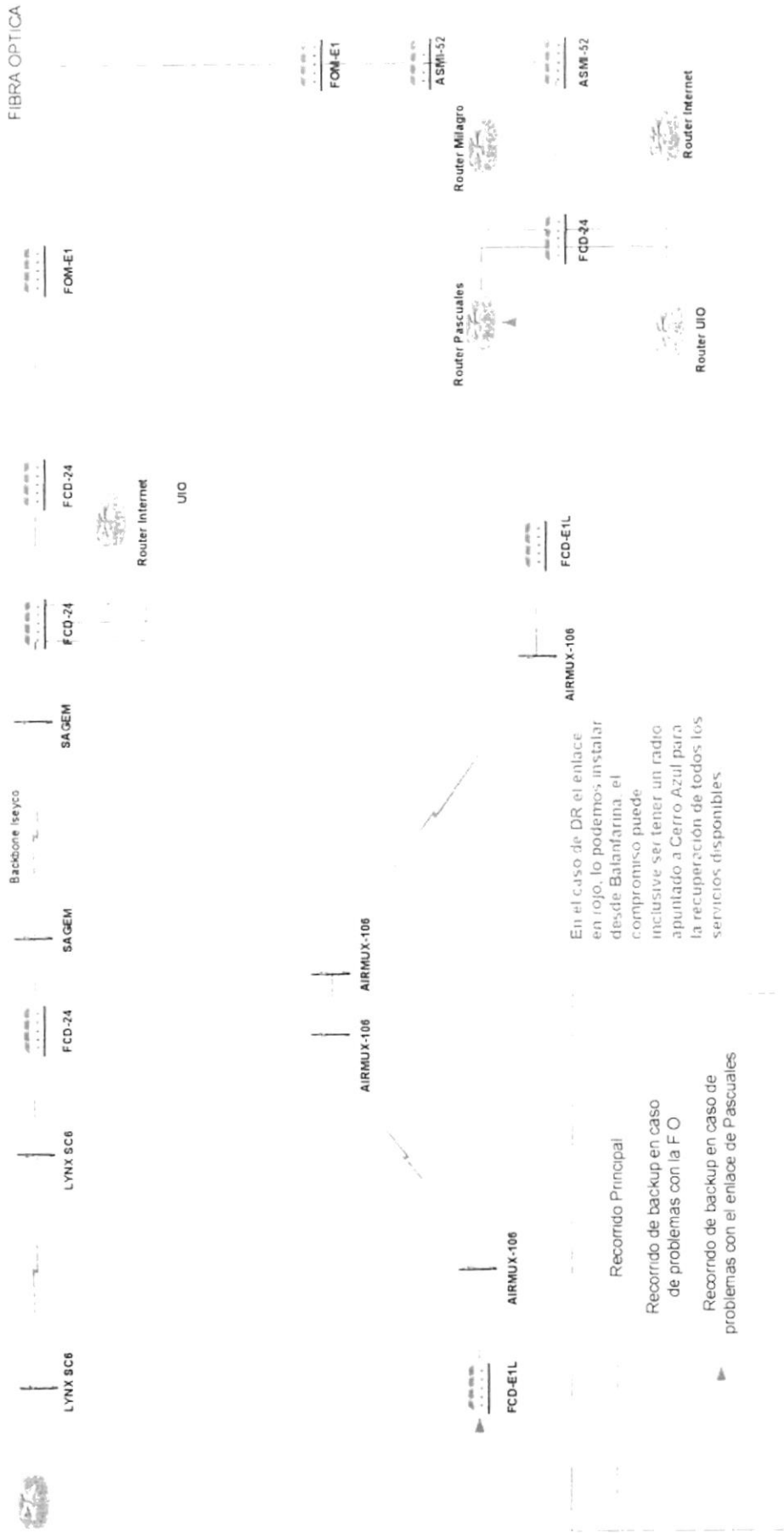
Sys@dmin com. S.A.	Carlos Cruz	2-515519	2-305900	099-945453	Vélez 409 y Escobedo 1er Piso	Reordenamiento de líneas de ingreso a la Central	
Telesis S.A.	Ing. Víctor Salguero	2-306911 / 2- 567201	2-308557		L. De Garaicoa 732 y V.M. Rendón 3er Piso of. 31	Servicios para la Central telefónica	
Xerox del Ecuador S.A.	Edmundo Merizalde A.	2-693440 / 2- 693450	2-693460	094-251075	Edif. Centrum piso 14 ofic. 4- Av. Fco. De Orellana Al. Bor.	Servicio de copias	edmundo.merizalde@ec.xaco.x erox.com

ANEXO D:

DIAGRAMA Y CONFIGURACIÓN DE COMUNICACIONES

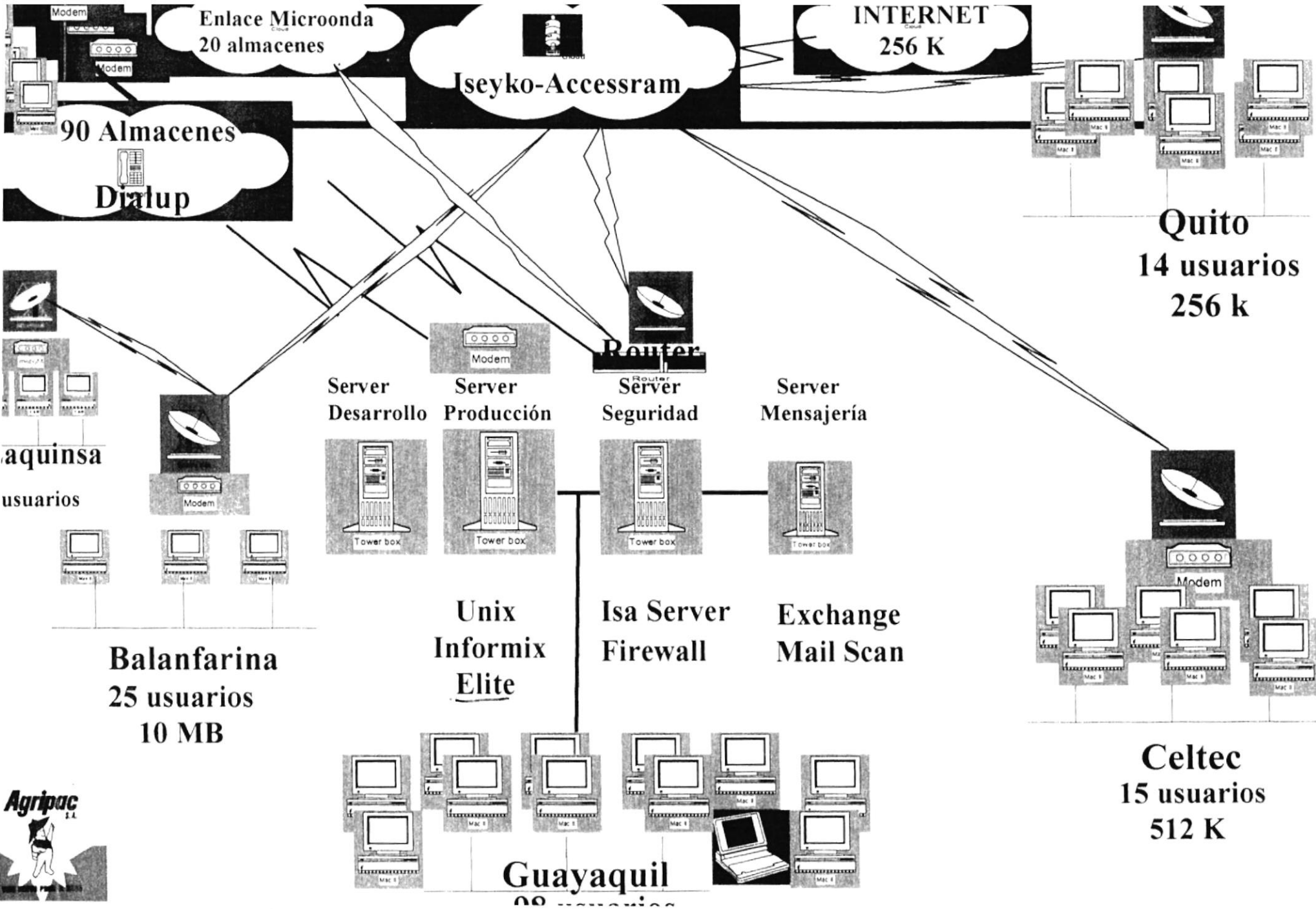
Red de Contingencia de Agripac S.A.





En el caso de DR el enlace en rojo, lo podemos instalar desde Balanfarma, el compromiso puede inclusive ser tener un radio apuntado a Cerro Azul para la recuperación de todos los servicios disponibles

- Recorrido Principal
- Recorrido de backup en caso de problemas con la FO
- Recorrido de backup en caso de problemas con el enlace de Pascauales



Enlace Microonda
20 almacenes

INTERNET
256 K

Iseyko-Accessram

90 Almacenes
Dialup

Quito
14 usuarios
256 k

Router

Server
Desarrollo

Server
Producción

Server
Seguridad

Server
Mensajería

aquinsa
usuarios

Modem

Tower box

Tower box

Tower box

Tower box

Balanfarina
25 usuarios
10 MB

Unix
Informix
Elite

Isa Server
Firewall

Exchange
Mail Scan

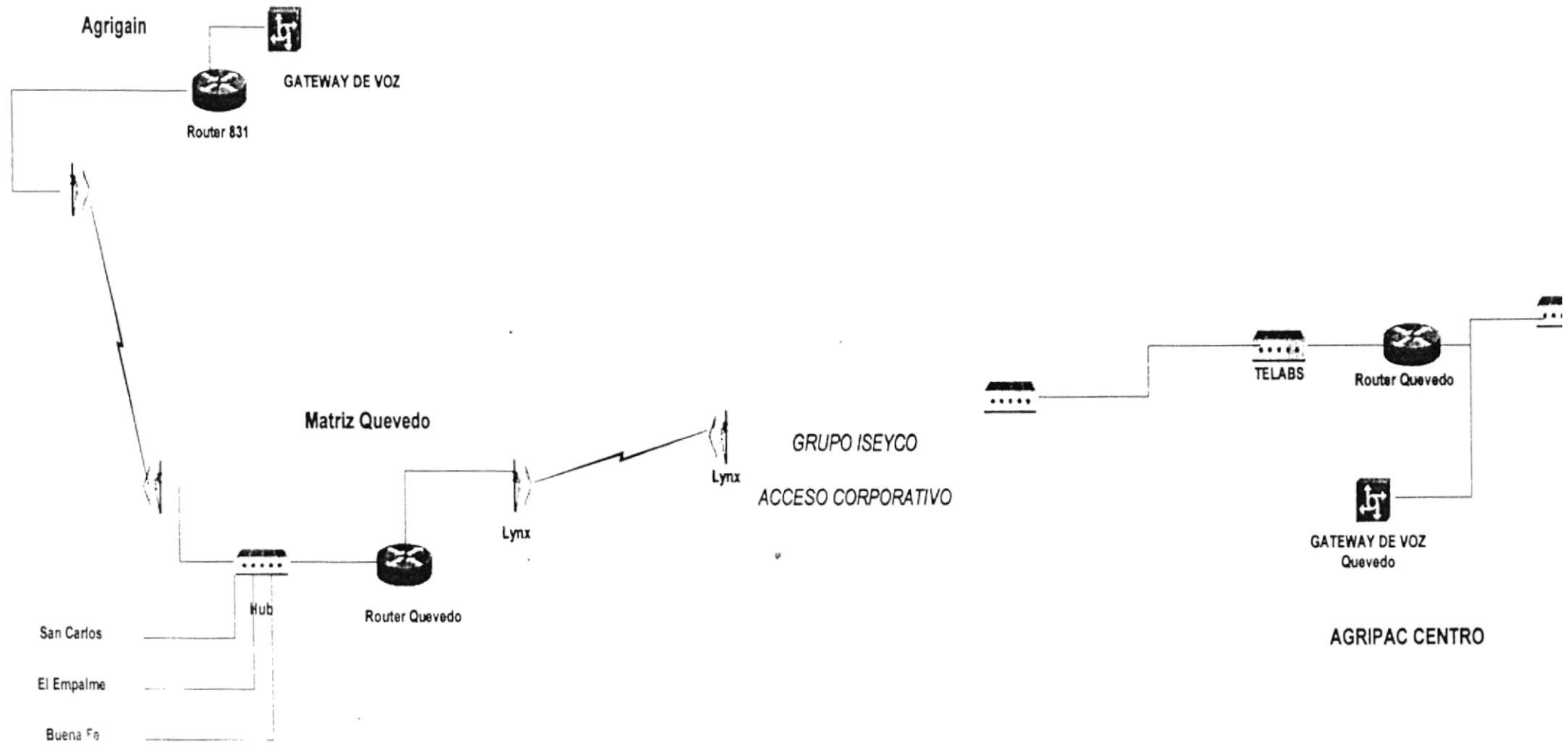
Modem

Celtec
15 usuarios
512 K

Guayaquil
00 usuarios

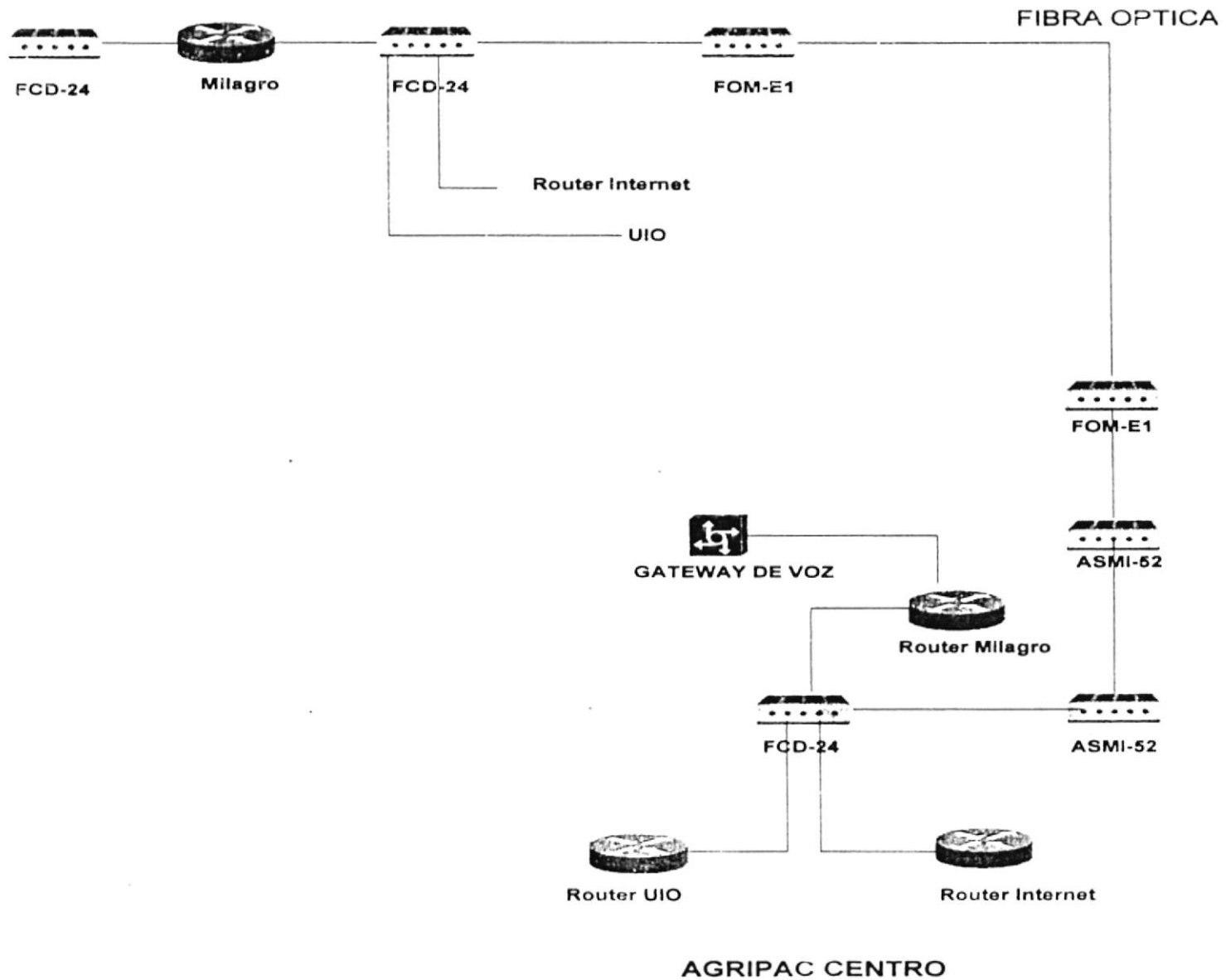


RED AGRIPAC QUEVEDO

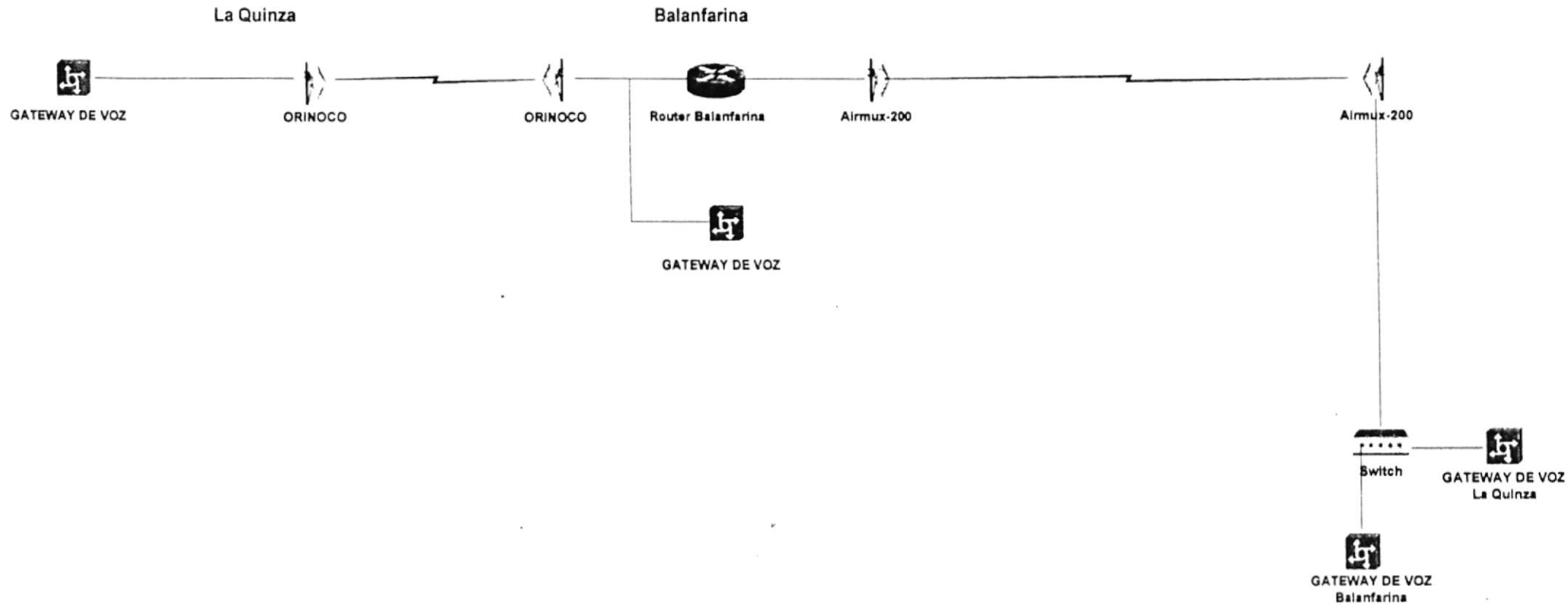


RED AGRIPAC MILAGRO

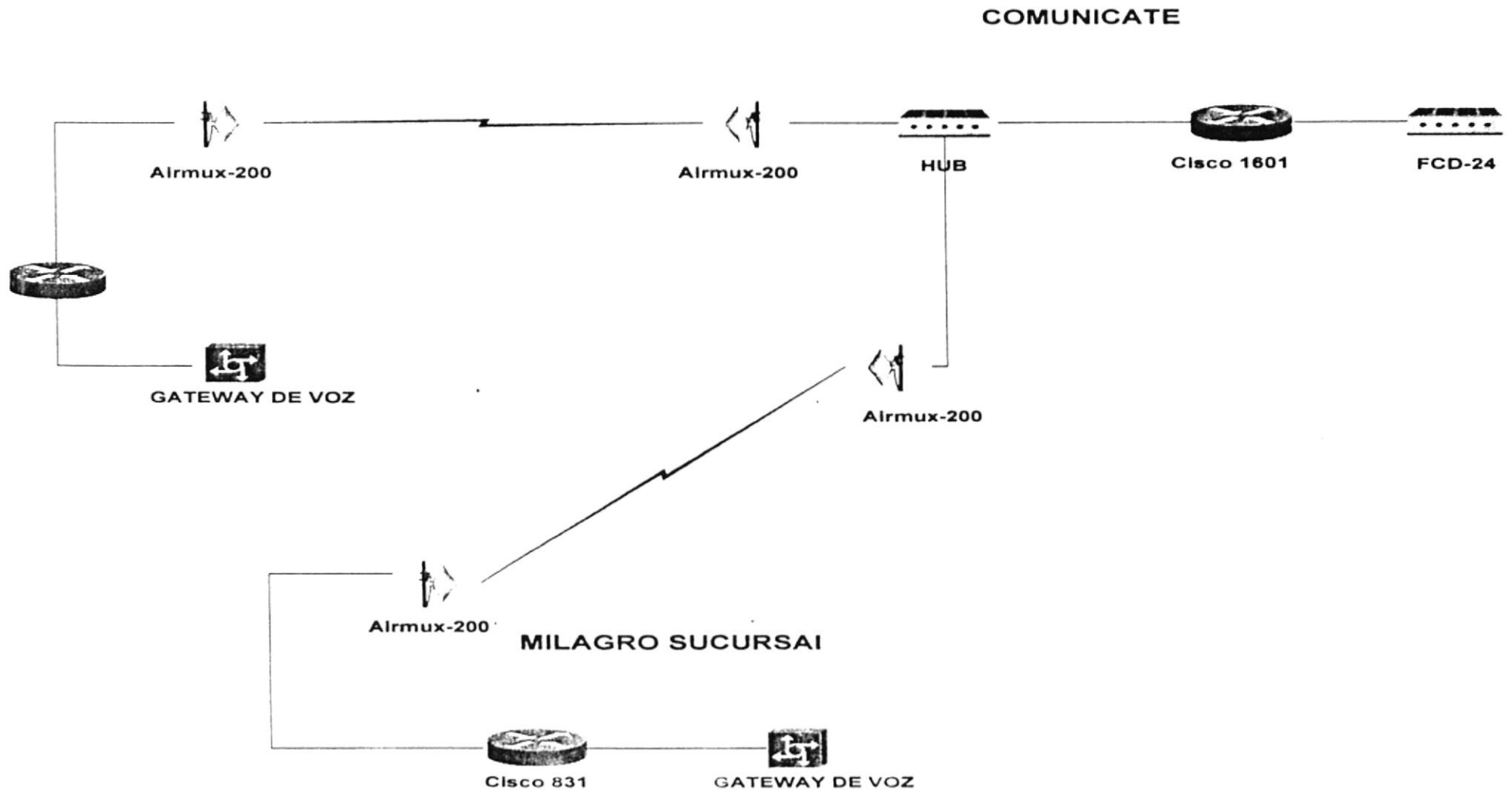
MEGADATOS



RED AGRIPAC BALANFARINA, LA QUINZA



RED AGRIPAC MILAGRO



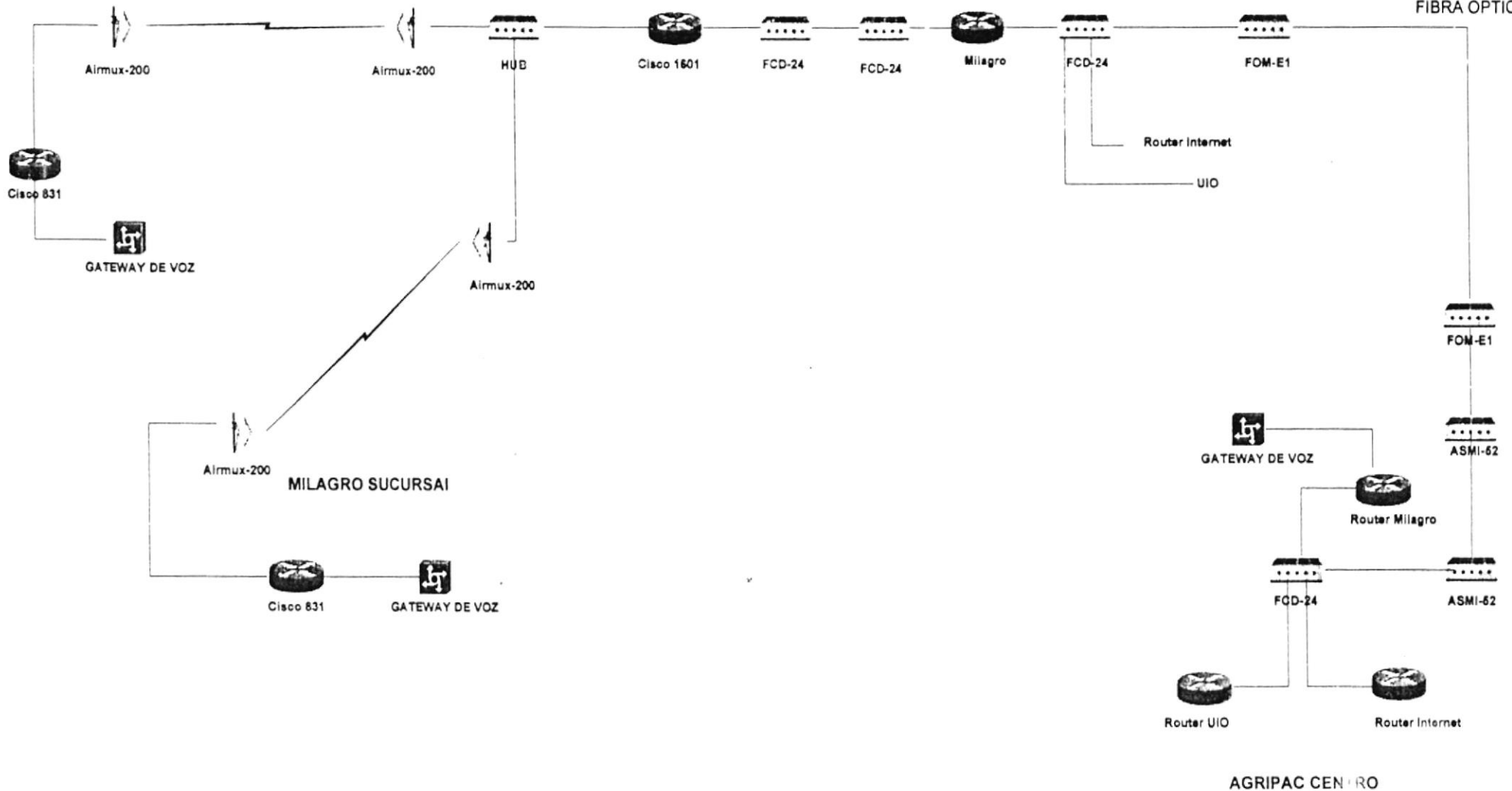
RED AGRIPAC MILAGRO

MILAGRO CENTRO

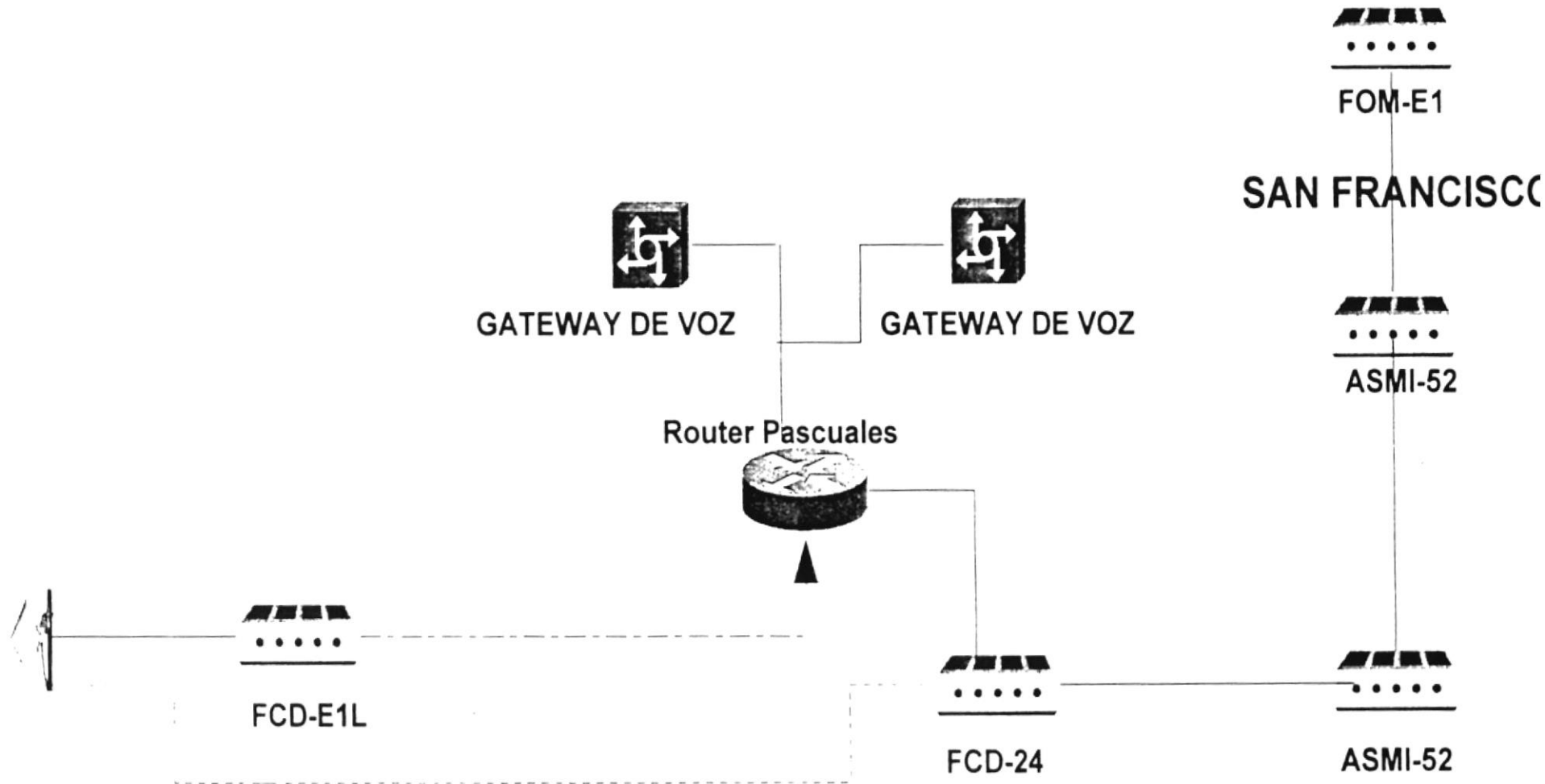
COMUNICATE

MEGADATOS

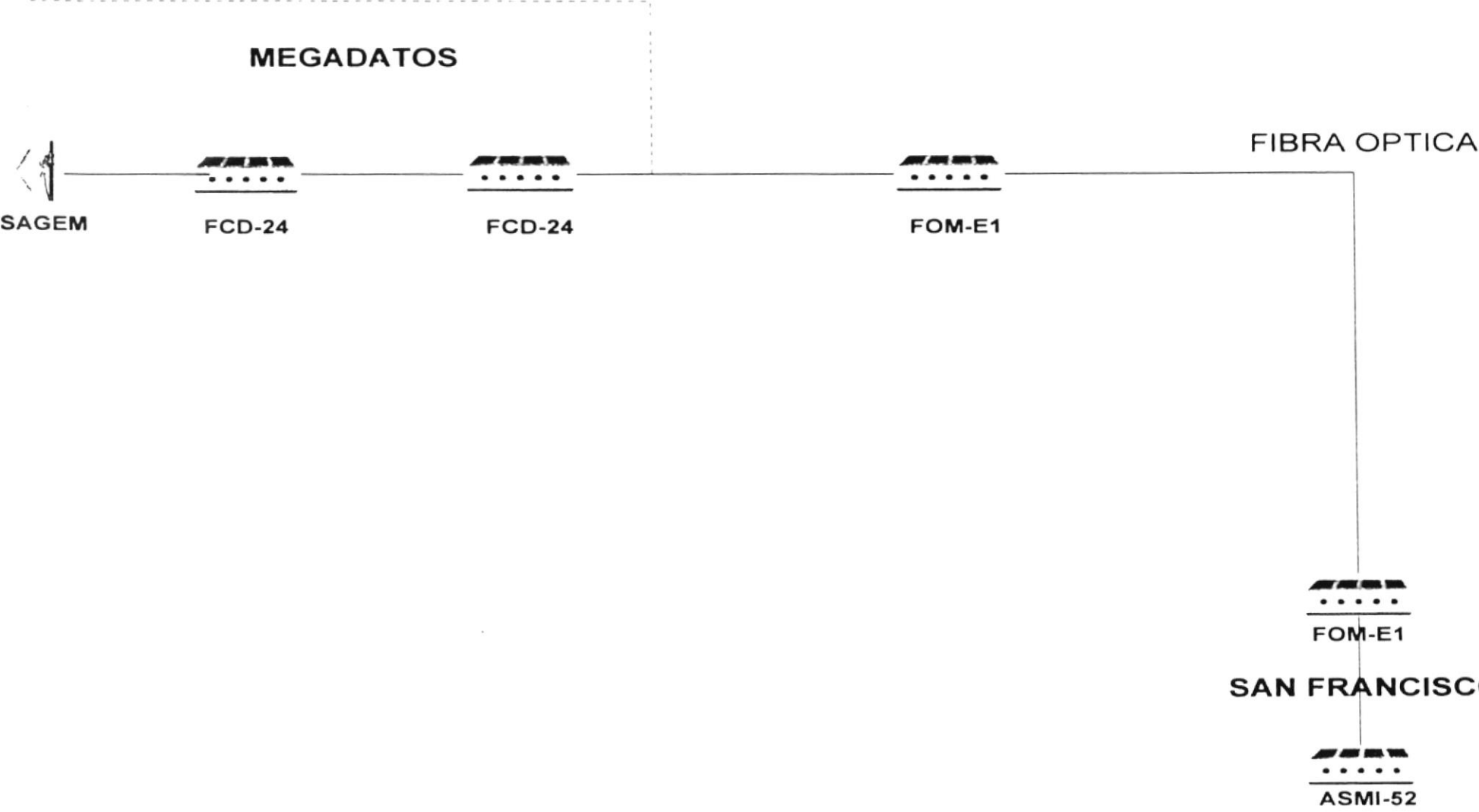
FIBRA OPTICA



RED AGRIPAC PASCUALES



RED AGRIPAC PASCUALES



RED AGRIPAC PASCUALES

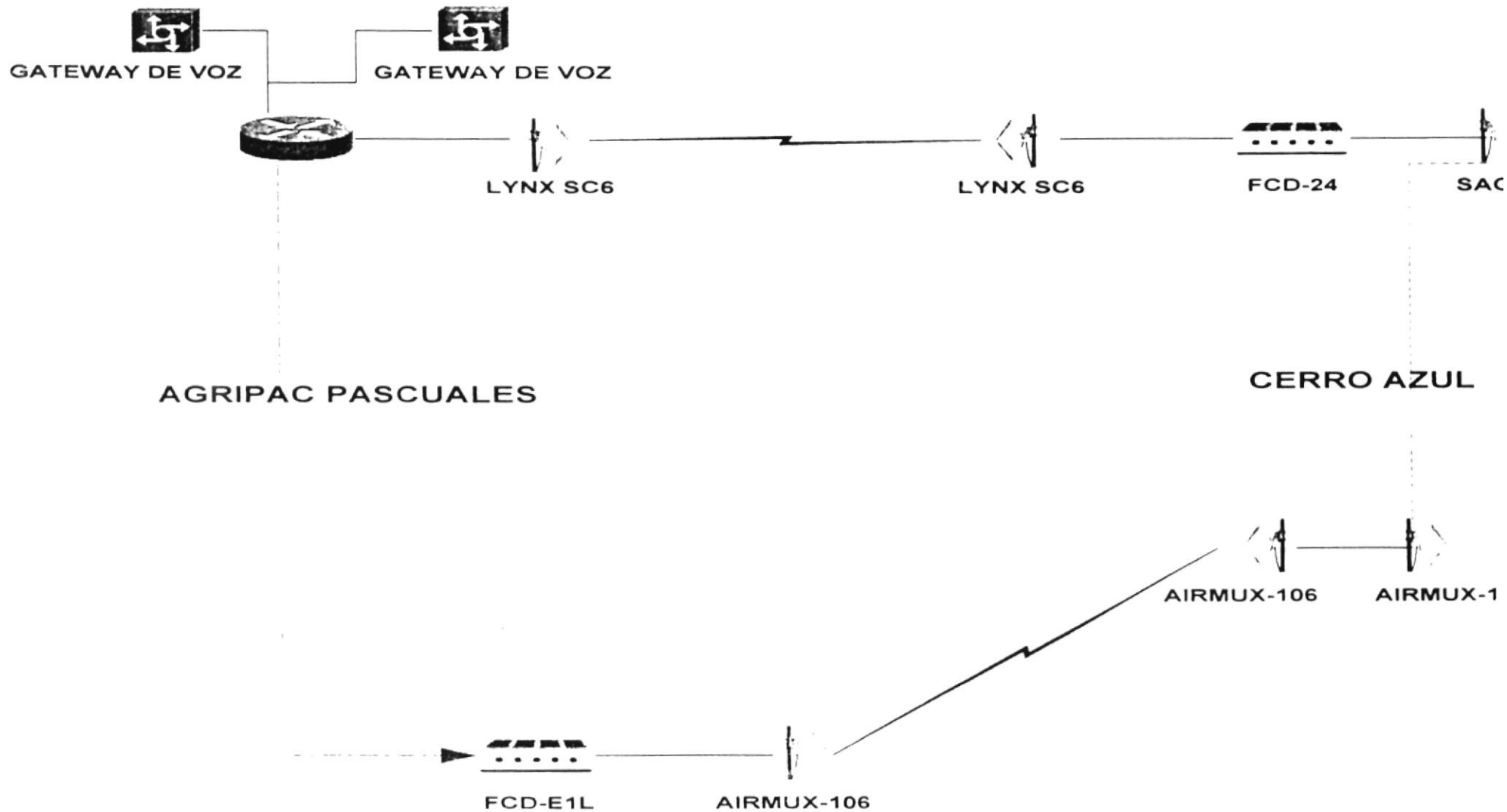
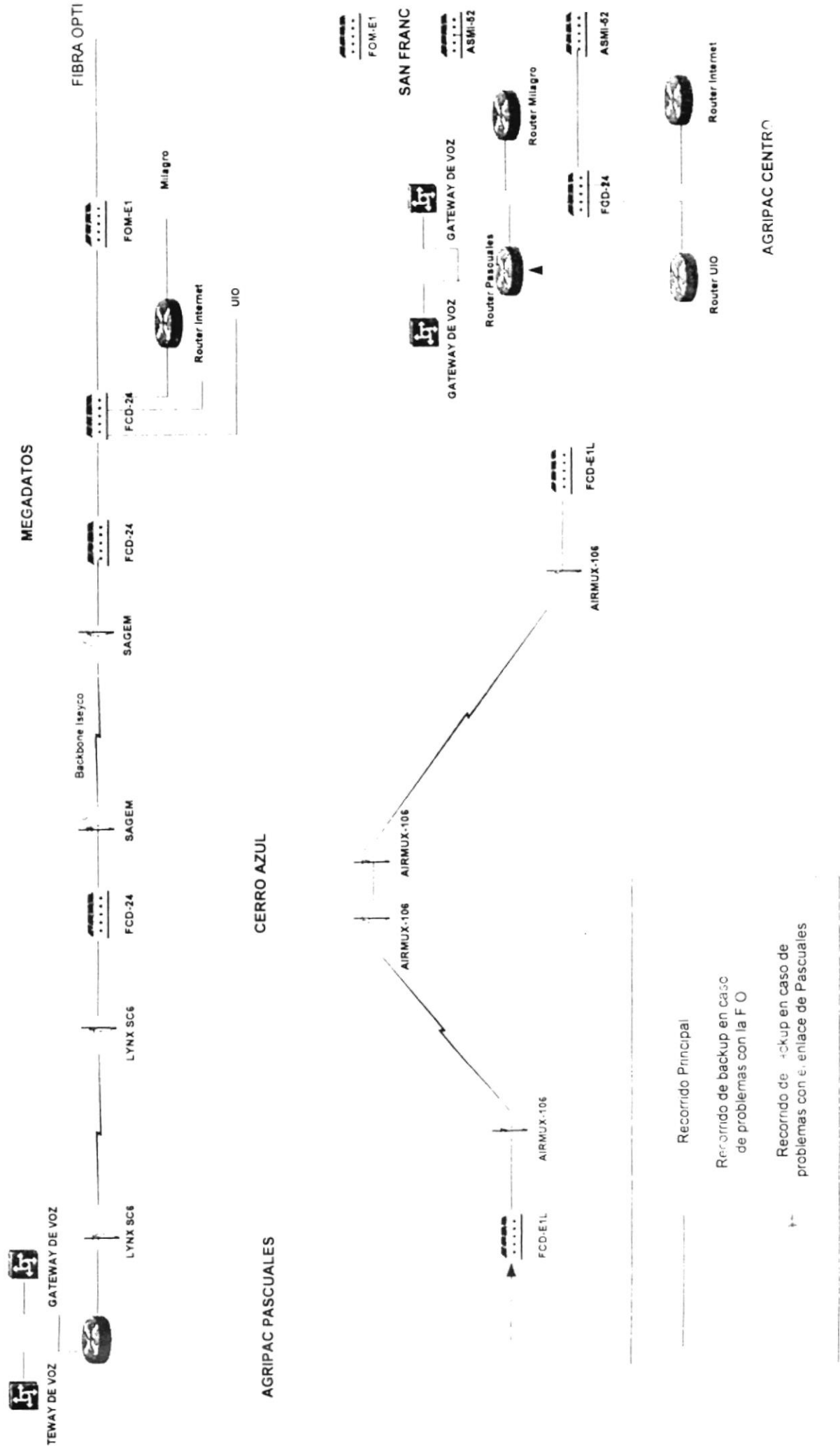


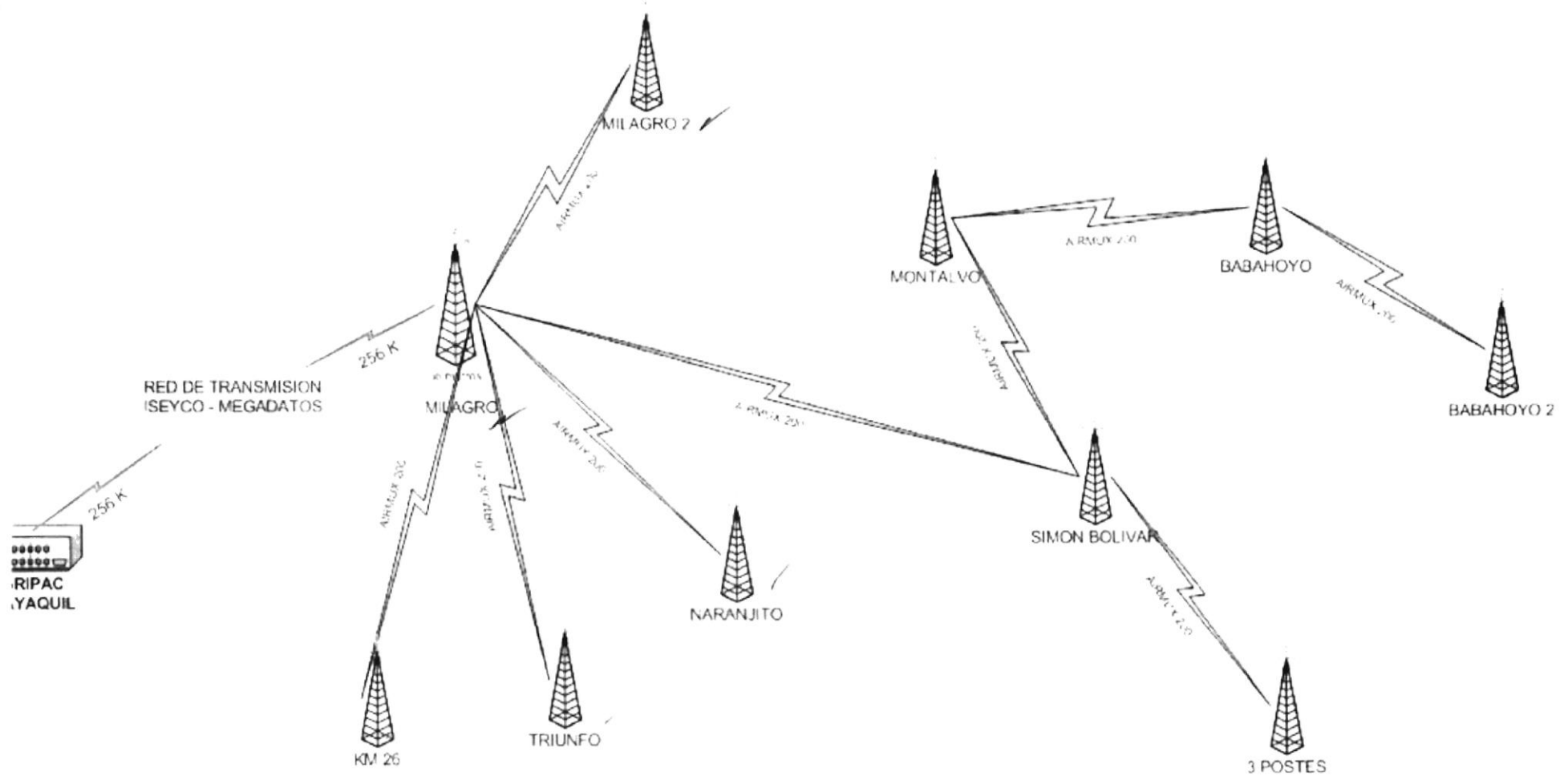
DIAGRAMA DE RED DE AGRIPAC





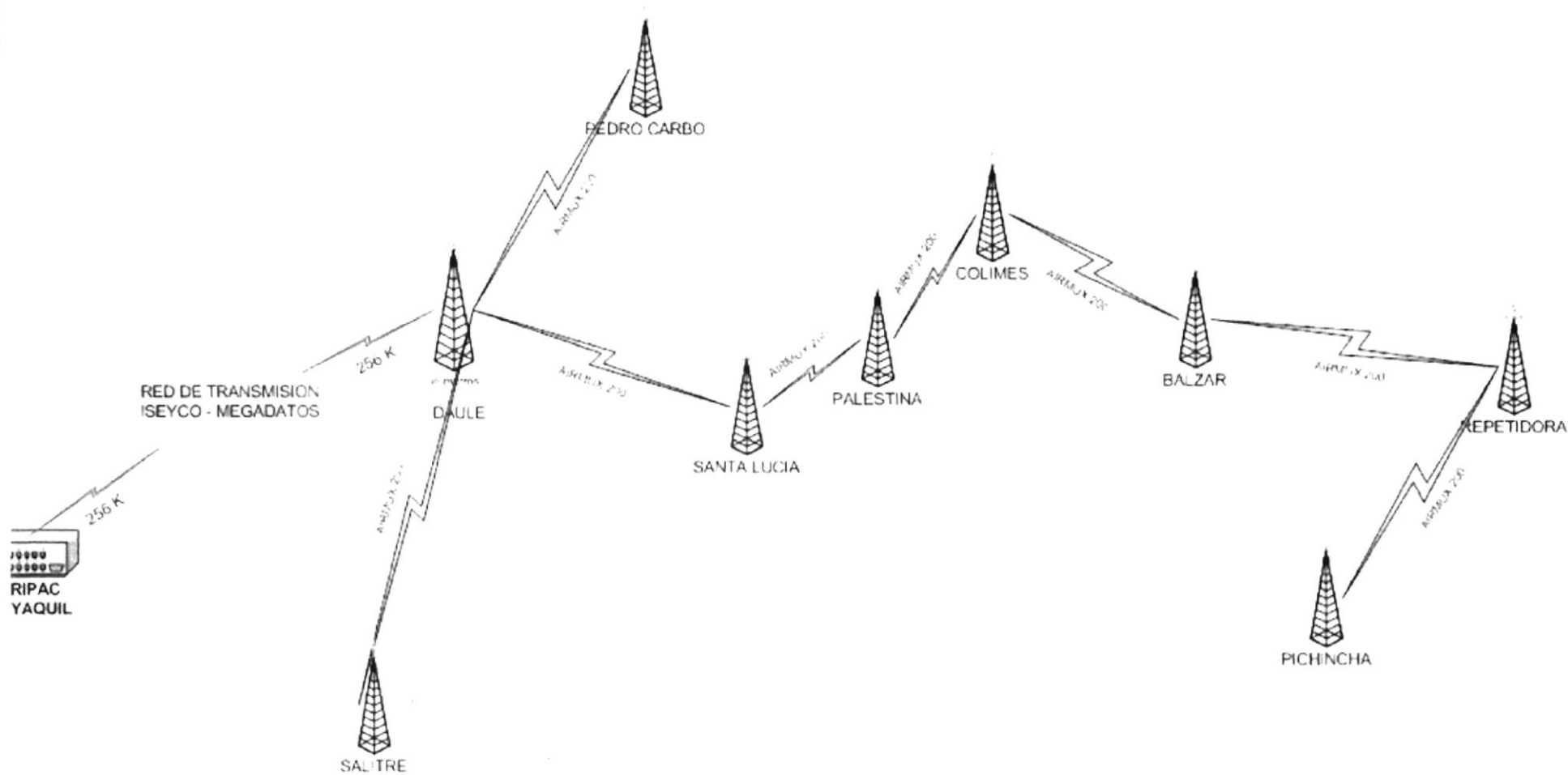
Comunicación en línea de Puntos de Ventas

Fase III Milagro



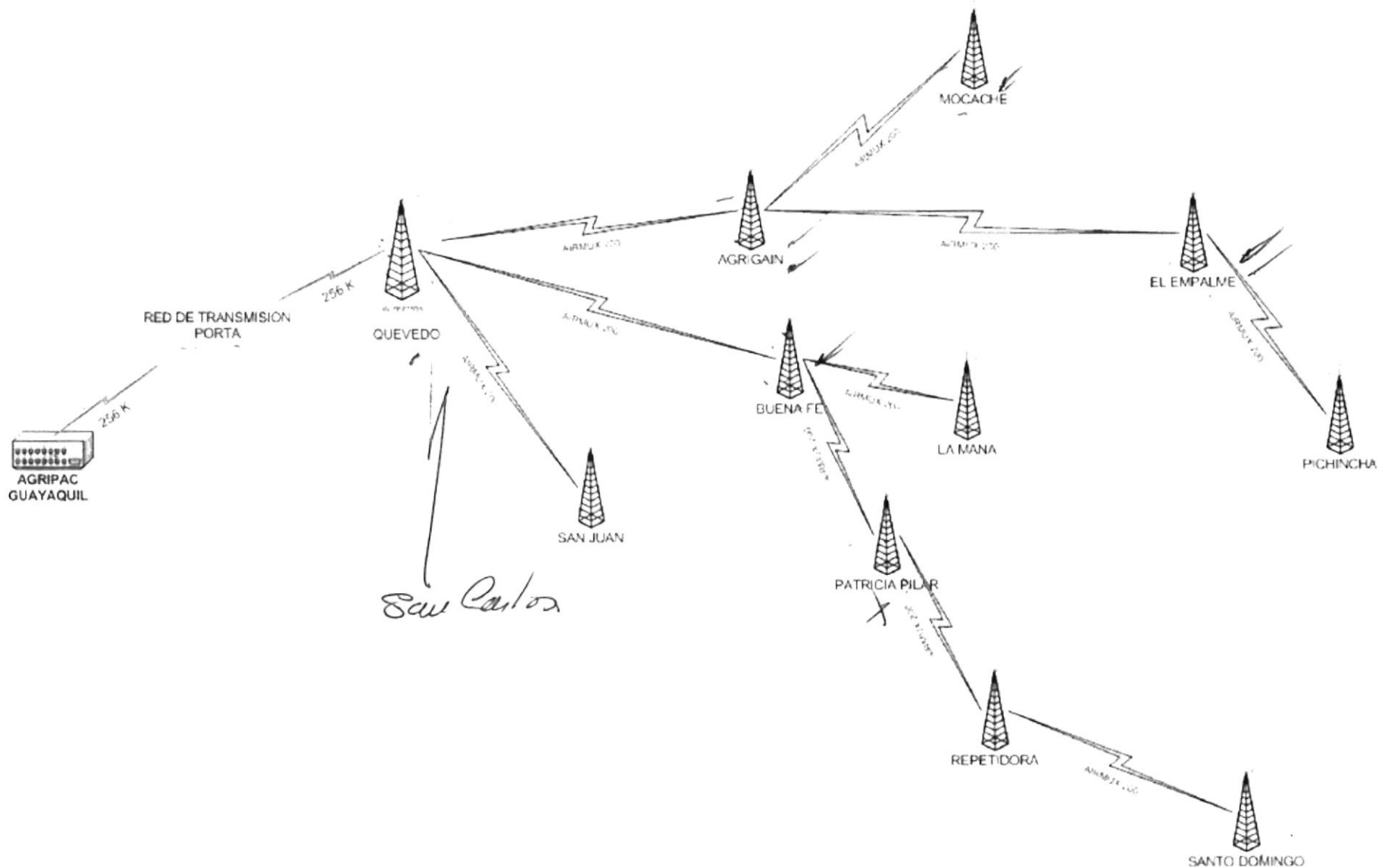
Comunicación en línea de Puntos de Ventas

Fase II Daule



Comunicación en línea de Puntos de Ventas

Fase I Quevedo



ANEXO E:

PROCESOS ALTERNOS MANUALES

DESCRIPCION DE LOS PROCESOS ALTERNOS Y MANUALES

Para efecto de este Plan de continuidad del Negocio BCP, de acuerdo al análisis de riesgos realizado BIA, enfocado a los procesos soportados fuertemente por los sistemas de información y tecnología IT, se determinaron que los procesos críticos del negocio visto desde un enfoque tecnológico son los siguientes:

- Proceso de Facturación
- Proceso de Producción
- Proceso de Crédito y Cobranzas
- Proceso de Inventario
- Proceso de Abastecimiento

Todos estos procesos son soportados en un alto porcentaje por sistemas y comunicaciones, pero además de la tecnología obligatoriamente requieren de otros recursos para su operatividad como son: Las personas, infraestructura, Maquinarias, Productos, Materia Prima y Vehículos.

Es importante manifestar que el 80 % de los puntos de ventas de la organización trabajan fuera de línea por estar ubicados geográficamente en las distintas ciudades del país, cada punto de venta utiliza para su control una aplicación desarrollada en cobol que funciona en un PC bajo Windows que le permite facturar, controlar el inventario, cuentas por cobrar, ventas y las guías de remisión (transferencia de mercadería entre almacenes), desde la oficina matriz se transfiere y/o envía tres veces por semana la información con los saldos nacional de clientes para que los puntos de ventas mantengan actualizada esta información sobre control de cupos de clientes, deuda vencida, cheques protestado, notas de debitos, notas de créditos, los cambios de precios, descuentos especiales y promociones son enviados vía correo electrónico, fax o boletines las transacciones generadas en esos puntos de ventas es transferida vía MODEM o medio magnético a la oficina matriz donde mediante una interfase que posee todos los controles requeridos es procesada e integrada a la aplicación central elite.

Los puntos de ventas y las plantas que están conectadas en línea a la matriz poseen esta aplicación como un proceso alternativo que debe ser utilizado cuando se produce una interrupción de las comunicaciones y/o paralización temporal del centro de cómputo.

Este proceso alternativo le permite a la organización mantener sus operaciones hasta 48 horas (promedio) después de una paralización del centro de cómputo, pasado ese tiempo resultaría inmanejable el negocio porque se perdería el control del inventario, saldos de clientes, control de cobranzas, control de la producción, habría un total descontrol en el abastecimiento, etc.

Al contar la organización con esos procesos alternos para mitigar los procesos críticos del negocio, se alargan los tiempos mínimos requeridos para que se habilite el centro de cómputo alternativo en caso de pérdida parcial o total de centro de cómputo o del edificio donde funciona.

El proceso alternativo descrito en los párrafos anteriores contribuye a mitigar el impacto y alargar el tiempo para activar el centro de cómputo alternativo ante una interrupción grave de los servicios de información y tecnología IT.

Los otros factores de quiebre de los procesos críticos como son: las personas, infraestructura, maquinarias, productos y vehículos tampoco se verían afectados en caso de un desastre que ocasione la destrucción parcial o total del centro de cómputo o de la infraestructura del edificio donde funciona el centro de cómputo porque los mencionados recursos están ubicados en las diferentes ciudades del país.

PROCESO ALTERNO MANUAL

La organización mantiene en todos los Punto de Ventas un proceso de ventas manual mediante la utilización de un formulario preimpreso (block) llamado "Egreso de Mercadería" que cuentan con la respectiva autorización del SRI, ese formulario se lo llena manualmente y es utilizado para realizar las ventas cuando se producen cortes prolongados de energía en cualquier punto de ventas. Posteriormente cuando se restablece la energía eléctrica es ingresado al sistema para la emisión de las facturas correspondiente, el formulario manual con la firma del cliente debe ser adjuntado obligatoriamente.

ANEXO F:

PROCEDIMIENTOS DE RECUPERACIÓN



SEGURIDAD – SALUD- AMBIENTE

PLAN DE RESPUESTA A CRISIS PRC

“ES MEJOR ESTAR PREPARADOS PARA ALGO QUE NO VA A
SUCEDER, A QUE NOS SUCEDA ALGO PARA LO QUE NO
ESTAMOS PREPARADOS”



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE
RESPUESTA A CRISIS
P.R.C.**

CONTENIDO

**SEGURIDAD
SALUD
AMBIENTE**

- 1.- INTRODUCCION Y GENERALIDADES.
- 2.- DESCRIPCION DE LA EMPRESA AGRIPAC S.A.
- 3.- PROCEDIMIENTOS ESPECIFICOS.
- 4.- DIAGRAMA DE FLUJO DEL PLAN OPERATIVO.
- 5.- PLANO GENERAL DE LAS INSTALACIONES.
- 6.- DESCRIPCION DE LAS ZONAS.
- 7.- MAPEO DE RIESGOS POR ZONAS.
- 8.- ORGANIZACIÓN DE LAS BRIGADAS.
- 9.- BRIGADA DE INCENDIO Y EVACUACION.
- 10.- BRIGADA DE COMUNICACIÓN Y COMANDO- PROCEDIMIENTOS.
- 11.- BRIGADA DE PRIMEROS AUXILIOS Y RESCATE-PROCEDIMIENTOS.
- 12.- ALTERACION DE ORDEN PÚBLICO.
- 13.- DESASTRES NATURALES: TERREMOTO, SISMO, INUNDACION.
- 14.- PROCEDIMIENTOS EN MANEJO RELACIONES PUBLICAS.
- 15.- TELEFONOS DE EMERGENCIA.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C**

**SEGURIDAD
SALUD
AMBIENTE**

1.- INTRODUCCION
GENERALIDADES

ESTE ES UN DOCUMENTO QUE CONTIENE UN CONJUNTO DE MEDIDAS, DISPOSICIONES Y PROCEDIMIENTOS A EJECUTARSE EN CASO DE PRODUCIRSE UNA EMERGENCIA.

*“TODA PERSONA QUE TRABAJA PARA **Agripac S.A** ES RESPONSABLE DE PROTEGER EL MEDIO AMBIENTE, LA SALUD Y LA SEGURIDAD DE NUESTRA GENTE, CLIENTES Y COMUNIDAD”*

Usted es la persona clave al planificar con anticipación y pensando siempre en realizar un trabajo seguro, que permita protegerse a UD. mismo, a los demás y a los bienes de la Empresa. Solo así.....ACTUARA Y TRABAJARA CON SEGURIDAD.

Considerando que su elemento humano constituye el factor más importante para su progreso y desarrollo, pone a la disposición de todos sus Empleados y Trabajadores su **Plan de Emergencias**.

1. INTRODUCCION.

Siendo una **EMERGENCIA** un evento que se presenta de manera súbita e inesperada y que podría originar daños a las personas, al medio ambiente y/o propiedad.

Pudiendo ser una **EMERGENCIA MAYOR** aquella que pone en peligro la vida de las personas, daño en el ambiente y/o a la propiedad requiriendo ayuda exterior y/o movilización completa de recursos.

o una **EMERGENCIA MENOR**, que sin poner en riesgo la vida de las personas, representa daños al ambiente y/o a la propiedad, estando dentro de la capacidad de control de la Empresa.

Es necesario contar con un Plan de Emergencia,


Por lo que

PARA AGRIPAC S. A

Un Plan de Emergencia o Autoprotección es la respuesta previamente planificada, que permitirá al personal, afrontar exitosamente cualquier emergencia individual o colectiva, provocada por la naturaleza o el hombre.

El Plan permite una mayor seguridad para el personal en caso de peligro inminente, contribuirá a disminuir las posibilidades de que la población sufra lesiones graves o irreparables durante una emergencia.

Se pueden generar SITUACIONES DE EMERGENCIA DE TIPO NATURALES como sismos, terremotos, inundaciones o PROVOCADAS POR EL HOMBRE como

 OFICINA PRINCIPAL GUAYAQUIL	PLAN DE RESPUESTA A CRISIS P.R.C	SEGURIDAD SALUD AMBIENTE
	1.- INTRODUCCION GENERALIDADES	

incendios, explosiones, derrames, atentados terroristas y fallas estructurales. Estas además de causar daño económico, pueden afectar en forma súbita y significativa el estado y condiciones de salud de las personas que se encuentran dentro de las instalaciones.

Para enfrentar adecuadamente una de las situaciones anteriores, por parte de los trabajadores, personal administrativo, contratistas, proveedores, visitantes, etc. es necesario, elaborar y poner en práctica un PLAN DE PREVENCIÓN Y CONTROL DE EMERGENCIAS.

Un Plan de Prevención y Control de Emergencias, requiere la cooperación y el apoyo decidido de todos los niveles organizacionales de AGRIPAC S.A.

PARA CUMPLIR CON LO ESTABLECIDO EN EL ART. 441 DEL CODIGO DE TRABAJO VIGENTE Y CON EL REGLAMENTO DE SEGURIDAD Y SALUD DE LOS TRABAJADORES Y MEJORAMIENTO DEL MEDIO AMBIENTE DE TRABAJO EXPEDIDO MEDIANTE DECRETO EJECUTIVO # 2393 PUBLICADO EN EL REGISTRO OFICIAL # 565 DEL 17 DE NOVIEMBRE DE 1986, SE REGLAMENTA LA ORGANIZACIÓN, FUNCIONAMIENTO Y FORMA DE LOS PROGRAMAS DE SALUD OCUPACIONAL QUE DEBEN DESARROLLAR LAS EMPRESAS INCLUYENDO LA ORGANIZACIÓN Y DESARROLLO DE UN PLAN DE EMERGENCIAS, TENIENDO EN CUENTA: PREVENCIÓN, PLAN ESTRUCTURAL Y DE CONTROL DE LAS EMERGENCIAS.

El presente Plan se fundamenta en la estructuración de Acciones Preventivas y de preparación administrativas, funcionales y operativas; antes y después de una Emergencia, que permita a la Empresa adaptarse a las condiciones reales de sus amenazas, creando condiciones que permitan a las personas que laboran, adquirir los conocimientos y actitudes organizativas necesarias para actuar correctamente en la Prevención y el control de las Emergencias.

2. JUSTIFICACION.

Diseñar Programas y actividades para la Prevención y Preparación de Emergencias, al igual que la formación de Brigadas de Salud y Seguridad que involucren conceptos nuevos para que este proceso sea cada vez mas integro, está por demás justificado.

Es evidente que una situación de Emergencia necesita un manejo que se puede salir de los procedimientos normales de una organización y requiere la utilización de recursos internos y posiblemente externos, y ante todo contar con las herramientas y metodología eficientes que posibiliten la recuperación en el menor tiempo posible de las personas y bienes afectados.

Con el Plan de Emergencia se pretende minimizar las consecuencias y severidad de los posibles eventos emergentes que puedan presentarse en un área o sector determinado; disminuyendo el daño que se pueda presentar en las personas, como a nivel económico de la Empresa.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C**

1.- INTRODUCCION
GENERALIDADES

**SEGURIDAD
SALUD
AMBIENTE**

El logro de los objetivos de los Planes de Contingencias y los Programas que desarrolle el equipo y las Brigadas, no están dados solamente por el nivel de Capacitación técnica y profesional de quienes la ejecutan, sino además por el desarrollo humano y la concepción del trabajo en equipo que posea el personal de la Empresa.

3. OBJETIVO GENERAL.

Establecer Procedimientos, generar destrezas, condiciones que les permitan a los funcionarios y empleados, Prevenir, Protegerse en caso de desastres o amenazas colectivas que pongan en peligro su integridad y la del personal visitante en determinado momento, mediante acciones rápidas, coordinadas y confiables.

Evacuar al personal por y hasta lugares de menor riesgo y en caso de presentarse lesionados contar con una estructura organizativa para brindarles una primaria y adecuada atención en salud.

4. OBJETIVOS ESPECIFICOS.

- ✓ Identificar y aplicar un proceso de planeación en Prevención, Mitigación, Atención y Recuperación en casos de emergencias y Desastres que se puedan presentar en la Empresa.
- ✓ Contar con una eficiente y adecuada estructura organizativa para casos de Emergencia.
- ✓ Estructurar un procedimiento normalizado de Evacuación para todos los usuarios y ocupantes de las instalaciones (operarios, empleados, contratistas, visitantes).
- ✓ Establecer un esquema operativo propio para la atención de posibles lesionados.
- ✓ Generar en los empleados involucrados condiciones de seguridad y sensibilizarlos para lograr su participación en las acciones de Prevención de Emergencias, alcanzando una eficiente organización, preparación, equipamiento, y práctica para adquirir la destreza necesaria de la Brigada, a fin de que cuando enfrenten una real emergencia, reaccionen individualmente y como grupo, de manera inmediata y favorable.
- ✓ Que el personal identifique las tareas que le corresponderá cumplir en la ejecución del plan y la importancia de su participación en todas las fases que llevan su aplicación.
- ✓ Estructurar y aplicar un programa de señalización para emergencias.

EN CONCLUSION.....EL PLAN DEBE ESTAR ORIENTADO A:

- SALVAR VIDAS.
- EVITAR DAÑOS AMBIENTALES.
- EVITAR PERDIDA DE BIENES.
- CONTROLAR O DETENER EL INCIDENTE EN EL MENOR TIEMPO POSIBLE.
- REHABILITAR LAS OPERACIONES



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C**

**SEGURIDAD
SALUD
AMBIENTE**

1.- INTRODUCCION
GENERALIDADES

POR LO TANTO ES NECESARIO:

- Conformar un equipo de manejo de crisis.
- Establecer procedimientos de actuación.
- Determinar las acciones a tomar en las diversas emergencias posibles.
- Permitir una respuesta rápida, segura y efectiva.
- Mantener una continua preparación a través de entrenamientos, simulacros, ejercicios.

5. COMPROMISO DE AGRIPAC S.A.


- ✓ Eliminar accidentes e incidentes ambientales.
- ✓ Reducir emisiones y desperdicios.
- ✓ Utilizar efectivamente la energía y otras fuentes naturales.
- ✓ Estar preparados para responder a emergencias.
- ✓ Evaluar nuestros productos y educar a nuestros empleados, clientes y al público sobre su responsabilidad con el medio ambiente, la salud y la seguridad.
- ✓ Ayudar a nuestros empleados, contratistas, compañeros de negocios y proveedores a entender, como sus acciones influyen en el desarrollo de las políticas de Seguridad, Salud y Ambiente.
- ✓ Continuamente mejorar nuestro desarrollo en Seguridad, Salud y Medio Ambiente a través de una gestión Gerencial efectiva.

6. DOCUMENTOS DISPONIBLES DURANTE UNA CRISIS.

- Plan de Respuesta a Crisis - Documento básico.
- Planos de las instalaciones, con las rutas de evacuación. Colocarlos en un lugar visible.
- Manual de normas y Procedimientos. Normas generales de Seguridad, Salud y Medio ambiente.
- Guía en el manejo de Relaciones Públicas con los Medios de Comunicación. Lista del Personal de la Planta, contratistas, clientes y visitantes. Listado de los teléfonos de los funcionarios, autoridades, hospitales, etc.
- Reporte de investigación de accidentes.

¿ QUE INFORMACION DEBE CONTENER EL PLAN DE EMERGENCIA?

- ✓ Descripción y plano de las instalaciones.
- ✓ Mapeo de Riesgos por zonas, posibles incidentes.
- ✓ Descripción del equipo contra incendio.
- ✓ Sistema de alarma.
- ✓ Descripción y conformación de las Brigadas.
- ✓ Procedimientos de actuación.
- ✓ Procedimientos de Salvamento y rescate.
- ✓ Procedimiento de conexión o interrupción de la fuente de energía.
- ✓ Diagrama de flujo operativo.

 OFICINA PRINCIPAL GUAYAQUIL	PLAN DE RESPUESTA A CRISIS P.R.C	SEGURIDAD SALUD AMBIENTE
	1.- INTRODUCCION GENERALIDADES	

- ✓ Señalización y vías de evacuación. Áreas de concentración.
- ✓ Números telefónicos del Gerente de la Planta, del Cuerpo de Bomberos, del Médico, de los Hospitales, Servicio de Ambulancia, Defensa Civil, de la Policía y de las autoridades del sector.

7. REQUERIMIENTOS

- ✓ Capacitar al personal en todo lo referente al plan de evacuación y sistemas de alarma.
- ✓ Verificar periódicamente que los extintores estén cargados y operativos.
- ✓ Mantener siempre despejadas y limpias las vías de evacuación primarias y secundarias, así como puertas de emergencia.
- ✓ Realizar simulacros de evacuación por lo menos una vez al año.
- ✓ Estos compromisos se suman a nuestras obligaciones básicas de cumplir con todas las leyes y regulaciones sobre seguridad, salud y medio ambiente.

8.- CAMPO DE ACCION DEL PLAN.

El presente plan está diseñado para los siguientes eventos, en las siguientes circunstancias:

Sismo / Terremoto.

Guayaquil y en general la Provincia del Guayas se encuentra en zona sísmica importante.


Incendio / Explosión / Derrames.

En cualquier área de las instalaciones, con posible origen en un corto circuito o fuego provocado por llamas abiertas, derrames en almacén o bodega, etc.

Alteración del Orden Público / Terrorismo.

Manifestaciones de carácter político que provoquen cierre de la vía principal.

Artefacto explosivo como carta, paquete en alguna zona de la Empresa .

 <p>OFICINA PRINCIPAL GUAYAQUIL</p>	<p>PLAN DE RESPUESTA A CRISIS P.R.C</p> <hr/> <p>1.- INTRODUCCION GENERALIDADES</p>	<p>SEGURIDAD SALUD AMBIENTE</p>
---	--	--

“ES MEJOR ESTAR PREPARADOS PARA ALGO QUE NO VA A
SUCEDER, A QUE NOS SUCEDA ALGO PARA LO QUE NO
ESTAMOS PREPARADOS”

EL PERSONAL ES NUESTRO RECURSO MAS IMPORTANTE, SU
SALUD, SEGURIDAD Y BIENESTAR SON NUESTRA MAYOR
RESPONSABILIDAD.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS.
P.R.C.**

**SEGURIDAD
SALUD
AMBIENTE**

2.- DESCRIPCION DE LA
EMPRESA

DESCRIPCION DE LA EMPRESA.

INFORMACIÓN GENERAL.

UBICACIÓN Y DESCRIPCION DE LAS

Agripac S. A (Oficina principal) está ubicada en la ciudad de Guayaquil Provincia del Guayas, al norte, en la calle General Córdova y Padre Solano; en el sector centro-comercial de la ciudad; siendo éstas las vías de acceso, existe un flujo normal de personas que transitan y vehículos que circulan.

Las instalaciones están dotadas y destinadas a Oficinas administrativas y a la distribución de productos agropecuarios, para ello cuenta con un almacén y bodega para dicho fines.

La estructura de las edificaciones está hecha de cemento armado con vigas de amarre de concreto, la cubierta con planchas de fibro-cemento, los pisos cubiertos con baldosas y cerámica.

Existen 4 edificios, 2 de ellos son altos, el uno cuenta con 3 pisos el cual se encuentra hacia la calle General Córdova, tiene dos accesos uno por la calle antes citada y el otro interior que da hacia el patio peatonal y vehicular y el otro interior de 4 pisos, que da hacia el área de parqueo y tránsito peatonal, no dispone de una salida directa a la calle. Las otras dos edificaciones son tipo villa de 2 plantas, la una da para la calle General Córdova y su entrada se encuentra en el área interna que da hacia el patio peatonal y vehicular, en ella funciona el Consulado Británico y la otra también da hacia la calle General Córdova pero el acceso igual da hacia el área de tránsito peatonal y vehicular interno, en ella funciona un comedor y habitaciones para hospedaje, se la conoce como villa Bandurria.

Las instalaciones se encuentran cercadas con muro de cemento.

A los lados y en la parte posterior se encuentran edificaciones para oficinas y viviendas todas ellas de cemento armado; al frente cruzando la calle se encuentra un solar vacío (parqueo vehicular privado) y edificaciones de igual manera para oficinas y viviendas.

El acceso o entrada principal a la edificación, para los empleados y público en general, se encuentra al frente de la misma sobre la vía principal (General Córdova); además dispone de 3 entradas y salidas adicionales en el frente sobre esta misma vía, las cuales se encuentran cerradas al acceso de vehículos y personas.

Cuenta con áreas verdes, área de parqueadero interior que servirían de salidas de evacuación en caso necesario.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS.
P.R.C.**

**SEGURIDAD
SALUD
AMBIENTE**

2.- DESCRIPCION DE LA
EMPRESA

ANTECEDENTES.

La Empresa en particular no ha tenido ningún antecedente de incendios, explosiones, derrames, etc. en sus instalaciones. En el tiempo de vida de la Empresa no se han presentado sismos, inundaciones; por lo tanto al momento no se puede precisar la resistencia de la construcción.

ASPECTOS ADMINISTRATIVOS.

El personal administrativo y de servicio es de alrededor 100 personas, de las cuales entre 10 a 15 no permanecen la totalidad de la jornada en los edificios. Se estima un flujo de personas entre clientes, visitantes, etc. entre 50 a 60 personas al día

En la Empresa, las actividades de Salud Ocupacional están bajo la responsabilidad del respectivo departamento, supervisado por un Médico especializado en Medicina del Trabajo.

Actividades de capacitación sobre temas de Salud Ocupacional se llevan a cabo según cronograma de actividades, resultado del Programa de Salud Ocupacional.

La Seguridad Civil de las instalaciones está encargada mediante contrato a Empresa privada de vigilancia, con tres guardias durante el día y durante la noche.

MAQUINARIA Y EQUIPOS.

En las oficinas administrativas se dispone de muebles y equipos necesarios para el buen desarrollo de las actividades como: computadoras, calculadoras, fax, impresoras, fotocopidora, escritorios, sillas, archivadores, cortinas plásticas, etc.

Existe un Almacén para la venta de productos agropecuarios, el cual tiene su entrada principal hacia la calle General Córdova y un acceso lateral dentro del área de circulación peatonal y vehicular interna. Una Bodega para el almacenamiento de productos agropecuarios sirve para abastecer al almacén y solo dispone de un inventario bajo de acuerdo a las necesidades del mismo.

POLITICA DE SALUD OCUPACIONAL.

Agripac S. A preocupada por la protección de sus empleados, trabajadores, visitantes, contratistas, proveedores y público en general, ante la amenaza de un incidente o accidente en los sitios de trabajo, estableció la política de mantener en operación el Comité y las Brigadas de Emergencia, suministrando a todos sus funcionarios el más alto grado de Seguridad y Salud para el desempeño de las tareas asignadas.

La Gerencia aportará el Liderazgo y los recursos necesarios que permitan cumplir cabalmente los objetivos estipulados en el Plan de Contingencia.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS.
P.R.C.**

**SEGURIDAD
SALUD
AMBIENTE**

2.- DESCRIPCION DE LA
EMPRESA

El uso apropiado de estas inversiones, nos permitirán cumplir la misión de Proteger, Prevenir y Minimizar los riesgos de operación.

Cada persona que integre el Comité y las Brigadas de Emergencia, debe reconocer y cumplir con responsabilidad el compromiso de integridad con los demás.

Cada miembro de la familia *Agripac S.A.*, debe estar comprometido a cumplir y apoyar las normas de Seguridad y Salud se promulguen.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

**SEGURIDAD
SALUD
AMBIENTE**

**3.- PROCEDIMIENTOS
ESPECIFICOS**

DISPOSICION GENERAL

El ingreso de personas ajenas a la Empresa solo puede ser autorizado por la Gerencia General o la persona que esté a cargo en ese momento.

El Plan de Emergencia siempre será activado por el Funcionario de más alta jerarquía que se encuentre al momento del incidente.

El Jefe del incidente (Gerencia General) podrá requerir de la totalidad del equipo de Emergencia o de solo una parte de él, dependiendo de la clase y magnitud del incidente.

CADENA DE RE-EMPLAZOS:

GERENCIA GENERAL → GERENCIA RECURSOS HUMANOS →
GERENCIA COMERCIALIZACIÓN → EMPLEADO MÁS ANTIGUO →
GUARDIANA.

SEGURIDAD FISICA

- ✓ La Seguridad física de las instalaciones, los equipos y productos allí almacenados será de responsabilidad del personal de vigilancia privada. Si la Emergencia obliga a evacuar equipos, documentos, archivos para ser instalados en otro sitio para continuar con las operaciones comerciales, será responsabilidad del Coordinador de Evacuación.

PROCESOS Y SERVICIOS PUBLICOS

- ✓ La parada total de la Empresa o alguna área en especial, es responsabilidad del Coordinador de la Brigada de Comunicación y Comando y su personal a cargo.
- ✓ Para la reactivación y normalización de las labores después de terminada la Emergencia se requiere la aprobación de la Gerencia.

PROPIEDADES Y COMUNICACIONES ADYACENTES


- ✓ Si el siniestro ocurrido dentro de las instalaciones de la Empresa afecta a propiedad o público vecino, deberá informarse a las autoridades y al sistema local de emergencias (911), siempre con la autorización de la Gerencia General. Deberá coordinarse acciones con ellos y evaluar la magnitud del daño y determinar de ser necesario la evacuación de las zonas vecinas.

OFICINAS E INSTALACIONES COMERCIALES ALTERNAS

- ✓ Si la Emergencia no permite el uso de las instalaciones de la Empresa, se deberá localizar oficinas comerciales alternas, bodegas en un lugar cercano a la Empresa.

RETORNO A OPERACIONES NORMALES

Debe inspeccionarse previamente para identificar los daños y evaluar las pérdidas, cerciorarse de las condiciones de seguridad de las instalaciones, de

 <p>OFICINA PRINCIPAL GUAYAQUIL</p>	<p>PLAN DE RESPUESTA A CRISIS P.R.C.</p> <p>3.- PROCEDIMIENTOS ESPECIFICOS</p>	<p>SEGURIDAD SALUD AMBIENTE</p>
---	--	--

ser favorable el Jefe del Incidente ordenará el retomo ordenado, rápido y seguro del personal, así como programará las operaciones de limpieza, la investigación del incidente y el retomo a las operaciones normales.

PAUTAS PARA EL PERSONAL EN GENERAL:

SI USTED.....DETECTA UNA SITUACION DE RIESGO:

Comuníquela inmediatamente a su Jefe y elabore el reporte de incidente.

SI DESCUBRE UN CONATO DE INCENDIO O ANOMALIA DE SEGURIDAD:

Comuníquese de inmediato con su Jefe y notifique a Guardianía.
Accione la alarma (si considera que el incidente es grave).

SI....ESTA ENTRENADO EN EL PLAN DE RESPUESTA A CRISIS:

- ✓ Únase a la Brigada respectiva y póngase a órdenes del Jefe de Brigada.
- ✓ Aliste extintores.
- ✓ Despeje el área para facilitar el ingreso.
- ✓ Combata el fuego (si está confinado en un solo sitio) con extintores PQS (Fuego de tipo general, con excepción del eléctrico) o CO2 (fuego de tipo eléctrico) de acuerdo al tipo de fuego.
- ✓ Ayude a evacuar al personal de la zona de riesgo.

SI.... ESTA OPERANDO CUALQUIER EQUIPO:

- ✓ Suspenda la labor que esté ejecutando.
- ✓ Apague o desconecte el equipo a su cargo y demás equipos eléctricos que observe que están prendidos.
- ✓ Busque al Coordinador de Evacuación y espere instrucciones.
- ✓ Ayude a sus compañeros a evacuar el lugar.
- ✓ Evite el pánico, no corra, no grite ni cause confusión.
- ✓ Camine rápido cerrando puertas y ventanas sin colocar el seguro.
- ✓ No transporte bultos.
- ✓ Conocer los dispositivos de seguridad e instalaciones de protección contra incendio.
- ✓ No regrese por ningún motivo al área de trabajo o al sitio del siniestro durante el proceso de evacuación.
- ✓ Cuando no se encuentre en su sitio de trabajo, únase al grupo del área respectiva.
- ✓ Si se encuentra acompañado de un visitante, contratista o proveedor, ayúdelo a utilizar la vía y salida de evacuación del área.
- ✓ En caso de la presencia de humo, desplácese a nivel del piso (agachado, gateando), el humo y los gases tóxicos pueden ser más peligrosos que el fuego.
- ✓ Antes de salir verificar el estado de las vías de evacuación.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

**SEGURIDAD
SALUD
AMBIENTE**

**3.- PROCEDIMIENTOS
ESPECIFICOS**

- ✓ Siga la ruta de evacuación según el plano y las indicaciones del Coordinador de Evacuación (se deben conocer las vías de evacuación y salidas de emergencia).
- ✓ Evitar riesgos innecesarios.
- ✓ Si se encuentra atrapado, colocar un trapo debajo de la puerta para evitar el ingreso del humo, manteniéndose agachado.
- ✓ Seguir las indicaciones del personal competente.
- ✓ Durante el recorrido permanezca unido al grupo y por ningún motivo se aleje.
- ✓ Dirijase al punto de reunión asignado y espere el conteo por parte del Coordinador y/o Jefe del área.
- ✓ Verifique la lista del personal en el punto de reunión final.

TENER SIEMPRE PRESENTE:

- Dejar cerrado cajones de escritorio y/o archivos.
- No obstaculizar vías de evacuación.
- Bajar las escaleras a paso ligero.

RECUERDE SIEMPRE LA UBICACIÓN DE :

- Salida de Emergencia.
- Extintores.
- Alarmas.

IMPORTANTE:

Personal de tesorería-contabilidad-caja, deberán ejercer tareas especiales tales como: cerrar cajas fuertes, archivos confidenciales, documentos de importancia.

RECUERDE:

- Si detecta un incidente que requiere atención, llamar a la extensión del Jefe del Plan de Emergencia o la persona que al momento haga sus veces (cadena de mandos).
- Los coordinadores de acuerdo a la Emergencia, pueden o no solicitar los servicios externos.
- La única persona que puede informar a los medios de comunicación y organismos gubernamentales es el Representante legal de la Empresa, nadie sin la debida autorización podrá hacerlo.

FIN DE EMERGENCIA

Es cuando la condición irregular ha sido controlada y la situación regresa a la normalidad.

Cuanto menor sea el tiempo en que se realiza la evacuación, mayores serán las posibilidades de éxito.

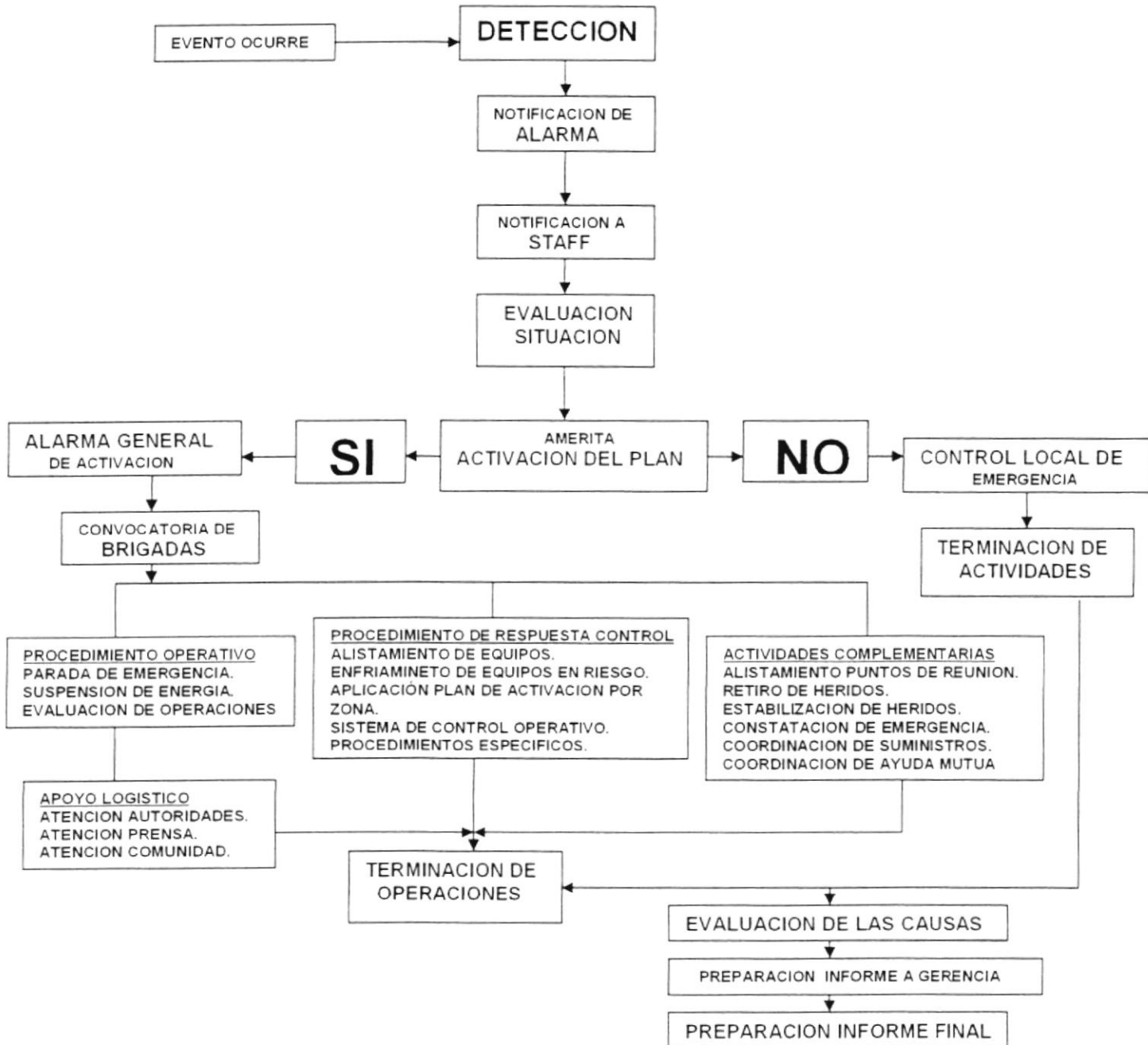


OFICINA PRINCIPAL
GUAYAQUIL

PLAN DE RESPUESTA A CRISIS P.R.C.

SEGURIDAD SALUD AMBIENTE

4.- DIAGRAMA DE FLUJO PLAN OPERATIVO



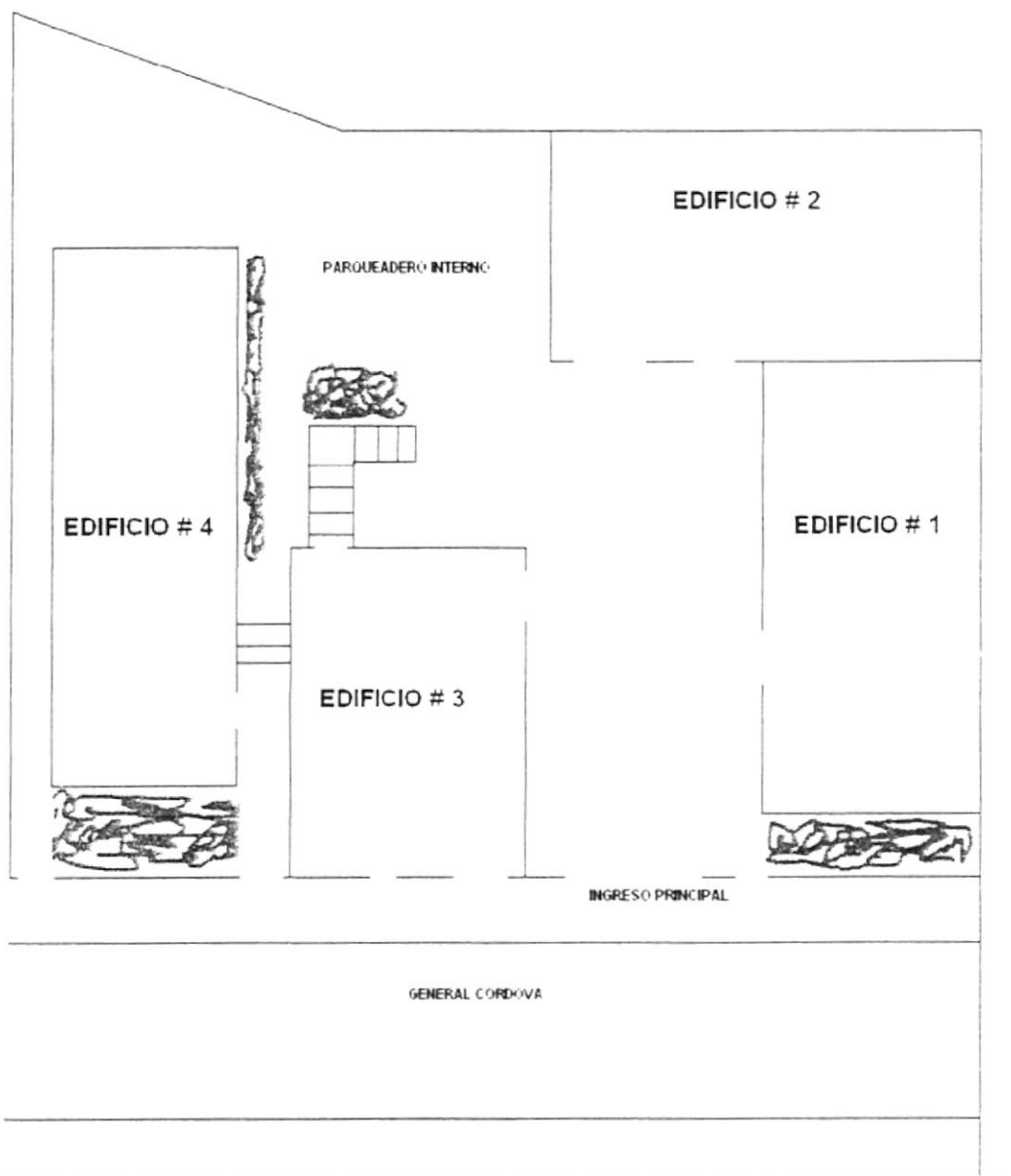



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

**SEGURIDAD
SALUD
AMBIENTE**

5.- PLANO GENERAL



 OFICINA PRINCIPAL GUAYAQUIL	PLAN DE RESPUESTA A CRISIS P.R.C.	SEGURIDAD SALUD AMBIENTE
	6.- DESCRIPCION DE LAS ZONAS	

Para una mayor observación de las situaciones y condiciones de Riesgo las instalaciones han sido divididas en 5 ZONAS

ZONA 1

EDIFICIO # 1
 VILLA CONSULADO

1A	PLANTA BAJA	
	GUARDIANA	(2 PERSONAS)
	RECEPCION / SUMINISTROS	(4 PERSONAS)
	CAJA	(1 PERSONA)
	CREDITO	(7 PERSONAS)
	BAÑOS	
	ESCALERA	
1B	PLANTA ALTA	
	GERENCIA GENERAL	(2 PERSONAS)
	CONSULADO / SECRETARIA	(3 PERSONAS)
	IMPORTACIONES	(3 PERSONAS)
	CORREDOR ACCESO AL EDIFICIO # 2	

ACCESOS Y SALIDAS:

ALTERNATIVA # 1: PUERTA PRINCIPAL

ALTERNATIVA # 2: EDIFICIO # 2 POR EL PRIMER PISO

ZONA 2

EDIFICIO # 2
 ADJUNTO EDIFICIO # 1

2 A	PLANTA BAJA	
	BODEGA ALMACEN	(2 PERSONAS)
	ESCALERA GENERAL	
2 B	PRIMER PISO	
	RECURSOS HUMANOS	(3 PERSONAS)
	BAÑO	
	NOMINA	(2 PERSONAS)
	CAFETERIA	(1 PERSONA)
2 C	GERENCIA FINANCIERA	(2 PERSONAS)
	BAÑO	
	SEGUNDO PISO	
2 D	AUDITORIA	(6 PERSONAS)
	TERCER PISO	
	CONTABILIDAD	(10 PERSONAS)
	CONTRALORIA	(2 PERSONAS)



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

**SEGURIDAD
SALUD
AMBIENTE**

6.- DESCRIPCION DE LAS
ZONAS

2 E CUARTO PISO
SISTEMAS (7 PERSONAS)
ALTILLO/ TALLER SISTEMAS

ACCESOS Y SALIDAS:

ALTERNATIVA #1: ESCALERA AL LADO DE LA BODEGA.

ALTERNATIVA #2: EDIFICIO # 1 POR EL PRIMER PISO

**ZONA 3 EDIFICIO # 3
HACIA LA CALLE G. CORDOVA**

3 A PLANTA BAJA
ALMACEN (3 PERSONAS)

3 B PRIMER PISO
ASISTENTE BANANO (1 PERSONA)
OFICINA DPTO. TECNICO (3 PERSONAS)
GERENCIA TECNICA BANANO. (1 PERSONA)
GERENCIA TECNICA CICLO CORTO. (1 PERSONA)
ASISTENTE CICLO CORTO. (1 PERSONA)
MERCADEO. (1 PERSONA)
ASISTENTE PUNTOS DE VENTAS. (1 PERSONA)
GERENCIA PUNTOS DE VENTA. (1 PERSONA)
BAÑOS.

3 C SEGUNDO PISO
GERENCIA COMERCIALIZACION. (1 PERSONA)
SECRETARIA. (1 PERSONA)
ETIQUETAS Y REGISTROS. (1 PERSONA)
ASISTENTE SEMILLAS. (1 PERSONA)
GERENCIA SEMILLAS. (1 PERSONA)
GERENCIA BANANO. (1 PERSONA)
ASISTENTE BANANO. (1 PERSONA)
BAÑOS.

3 D TERCER PISO
GERENCIA CONSUMO. (1 PERSONA)
ASISTENTE CONSUMO (1 PERSONA)
REPRESENTANTES CONSUMO (2 PERSONAS)
COMPRAS (2 PERSONAS)
CONTADOR HACIENDA (1 PERSONA)

ACCESOS Y SALIDAS:

ALTERNATIVA #1: ESCALERA PRINCIPAL HACIA LA CALLE.

ALTERNATIVA #2: ESCALERA POSTERIOR HACIA EL PARQUEO INTERIOR.

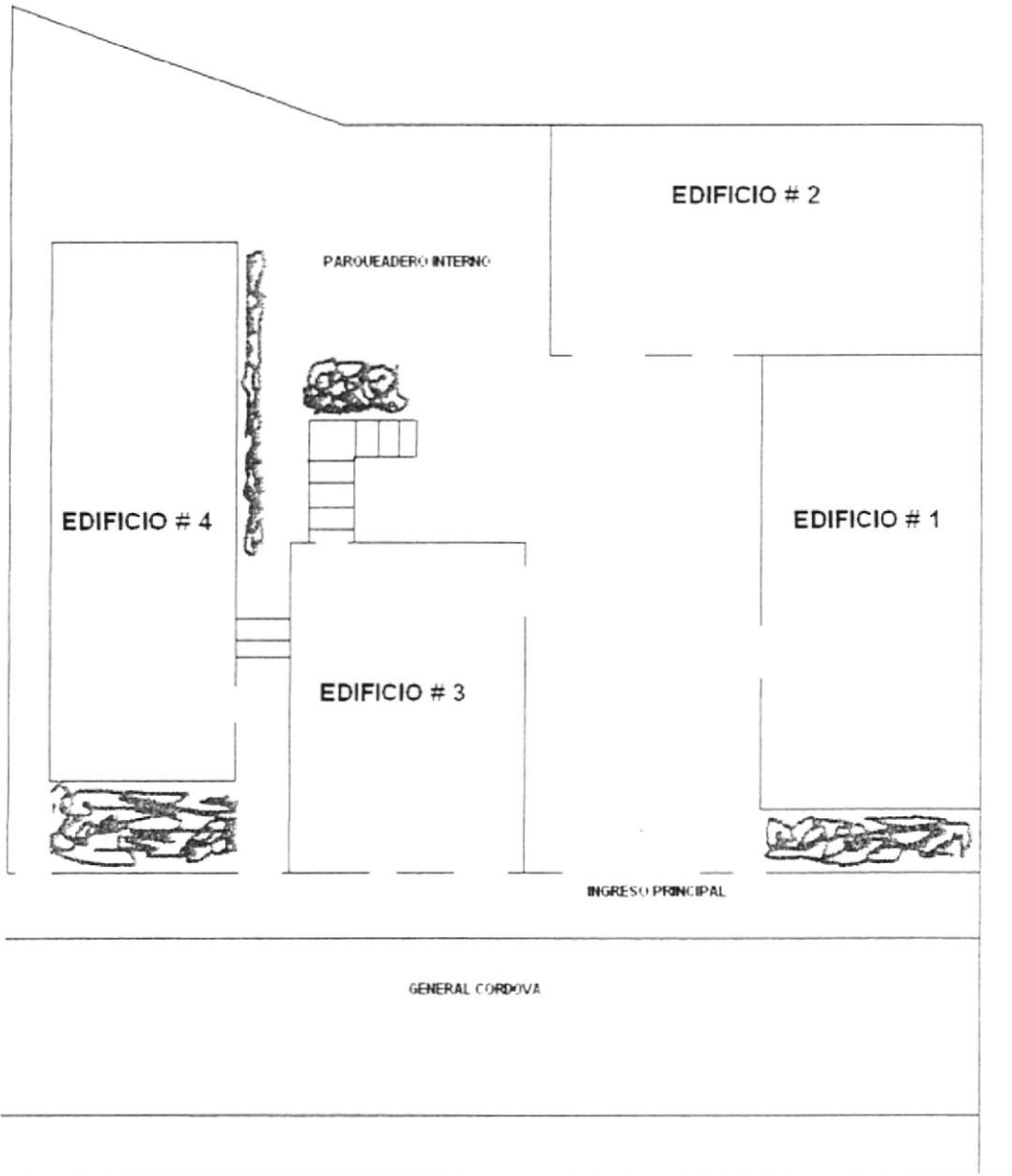


OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

**SEGURIDAD
SALUD
AMBIENTE**

6.- DESCRIPCION DE LAS
ZONAS





OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

**SEGURIDAD
SALUD
AMBIENTE**

7.- MAPEO DE RIESGOS

ZONA 1 EDIFICIO # 1 – VILLA CONSULADO

1A NIVEL DE RIESGO BAJO		
AREA:	RIESGO	CONTINGENCIA
PLANTA BAJA		
GUARDIANA / RECEPCION / SUMINISTROS / CAJA / DEPARTAMENTO TECNICO BANANO Y CICLO CORTO / BAÑOS / ESCALERA	<i>INCENDIO/ CORTO CIRCUITOS. SISMOS / ATENTADOS.</i>	<i>EQUIPO CONTRA INCENDIO. EQUIPO DE PRIMEROS AUXILIOS</i>

1B NIVEL DE RIESGO BAJO		
AREA:	RIESGO	CONTINGENCIA
PLANTA ALTA		
GERENCIA GENERAL / CONSULADO / SECRETARIA / IMPORTACIONES / CORREDOR ACCESO AL EDIFICIO # 2	<i>INCENDIO / CORTO CIRCUITO. SISMOS / ATENTADOS.</i>	<i>EQUIPO CONTRA INCENDIO EQUIPO PRIMEROS AUXILIOS</i>

ACCESOS Y SALIDAS:

ALTERNATIVA # 1: PUERTA PRINCIPAL

ALTERNATIVA # 2: EDIFICIO # 2 POR EL PASILLO DEL PRIMER PISO.

ZONA 2 EDIFICIO # 2 (ADJUNTO EDIFICIO # 1)

2A NIVEL DE RIESGO ALTO		
AREA	RIESGO	CONTINGENCIA
PLANTA BAJA		
BODEGA / ALMACEN AGROQUIMICOS. ESCALERA GENERAL	<i>INCENDIO CORTO CIRCUITO / CONTAMINACION / DERRAMES/ INUNDACION / SISMOS / ATENTADOS</i>	<i>EQUIPO PARA CONTROL DE RESIDUOS Y DERRAMES. EQUIPO PROTECCION PERSONAL EQUIPO DE CONTENCION. EQUIPO CONTRA INCENDIO. EQUIPO PRIMEROS AUXILIOS.</i>



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

7.- MAPEO DE RIESGOS

**SEGURIDAD
SALUD
AMBIENTE**

2B NIVEL DE RIESGO BAJO

AREA	RIESGO	CONTINGENCIA
PRIMER PISO		
COMPRAS / BAÑO / CAFETERIA / GERENCIA FINANCIERA/ BAÑO.	<i>INCENDIO. CORTO CIRCUITO. SISMOS / ATENTADOS</i>	<i>EQUIPO CONTRA INCENDIO. EQUIPO PRIMEROS AUXILIOS.</i>
FALTA		

2C NIVEL DE RIESGO BAJO

AREA	RIESGO	CONTINGENCIA
SEGUNDO PISO		
AUDITORIA	<i>INCENDIO. CORTO CIRCUITO. SISMOS/ ATENTADOS</i>	<i>EQUIPO CONTRA INCENDIO. EQUIPO PRIMEROS AUXILIOS.</i>

2D NIVEL DE RIESGO BAJO

AREA	RIESGO	CONTINGENCIA
TERCER PISO		
CONTABILIDAD. CONTRALORIA	<i>INCENDIO. CORTO CIRCUITO. SISMOS / ATENTADOS.</i>	<i>EQUIPO CONTRA INCENDIO. EQUIPO PRIMEROS AUXILIOS.</i>

2E NIVEL DE RIESGO BAJO

AREA	RIESGO	CONTINGENCIA
CUARTO PISO		
SISTEMAS. TALLER SISTEMAS (ALTILLO).	<i>INCENDIO. CORTO CIRCUITO. SISMOS / ATENTADOS.</i>	<i>EQUIPO CONTRA INCENDIO. EQUIPO PRIMEROS AUXILIOS.</i>

ACCESOS Y SALIDAS:

ALTERNATIVA # 1: ESCALERA AL LADO DE LA BODEGA
(PRINCIPAL DEL EDIFICIO).

ALTERNATIVA # 2: EDIFICIO # 1 POR EL PASILLO DEL PRIMER PISO.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

7.- MAPEO DE RIESGOS

**SEGURIDAD
SALUD
AMBIENTE**

ZONA 3 EDIFICIO # 3 (FRENTE CALLE G. CORDOVA)

3A <u>NIVEL DE RIESGO BAJO</u>		
AREA	RIESGO	CONTINGENCIA
PLANTA BAJA		
ALMACEN ESCALERA PRINCIPAL DEL EDIFICIO (ZAGUAN)	<i>INCENDIO. CORTO CIRCUITO. INUNDACION. DERRAMES. CONTAMINACION. SISMOS/ ATENTADOS.</i>	<i>EQUIPO PARA DERRAMES Y RESIDUOS. EQUIPO CONTRA INCENDIO. EQUIPO PRIMEROS AUXILIOS. EQUIPO PROTECCION PERSONAL. EQUIPO DE CONTENCION.</i>

3B <u>NIVEL DE RIESGO BAJO</u>		
AREA	RIESGO	CONTINGENCIA
PRIMER PISO		
DEPARTAMENTO DE CREDITO BAÑO. ASISTENTE PUNTOS DE VENTAS. GERENCIA PUNTOS DE VENTAS. BAÑO.	<i>INCENDIO. CORTO CIRCUITO. SISMO. ATENTADOS.</i>	<i>EQUIPO CONTRA INCENDIO. EQUIPO PRIMEROS AUXILIOS.</i>



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

**SEGURIDAD
SALUD
AMBIENTE**

7.- MAPEO DE RIESGOS

3C NIVEL DE RIESGO BAJO

AREA SEGUNDO PISO	RIESGO	CONTINGENCIA
GERENCIA COMERCIALIZACION. BAÑO. ASISTENTE GERENCIA. REGISTROS Y ETIQUETAS. ASISTENTE SEMILLAS. GERENCIA CICLO CORTO. GERENCIA BANANO. ASISTENTE BANANO. GERENCIA SEMILLAS. BAÑO.	<i>INCENDIO. CORTO CIRCUITO. SISMOS / ATENTADOS.</i>	<i>EQUIPO CONTRA INCENDIO. EQUIPO PRIMEROS AUXILIOS.</i>

3D NIVEL DE RIESGO BAJO

AREA TERCER PISO	RIESGO	CONTINGENCIA
GERENCIA CONSUMO ASISTENTE CONSUMO NOMINA RECURSOS HUMANOS CONTADOR HACIENDAS	<i>INCENDIO. CORTO CIRCUITO. ATENTADOS. SISMOS</i>	<i>EQUIPO CONTRA INCENDIO/ EQUIPO PRIMEROS AUXILIOS</i>

ACCESOS Y SALIDAS:

ALTERNATIVA#1: ESCALERA PRINCIPAL DEL EDIFICIO HACIA LA CALLE.

ALTERNATIVA#2: ESCALERA POSTERIOR HACIA EL PARQUEO INTERIOR.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

7.- MAPEO DE RIESGOS

**SEGURIDAD
SALUD
AMBIENTE**

ZONA 4 EDIFICIO # 4 VILLA BANDURRIA

4A NIVEL DE RIESGO MODERADO

AREA	RIESGO	CONTINGENCIA
PLANTA BAJA		
OFICINA ADMINISTRATIVA. COMEDOR. HABITACIONES. COCINA. BAÑOS	<i>INCENDIO. CORTO CIRCUITO. INUNDACION. SISMOS. ATENTADOS</i>	<i>EQUIPO CONTRA INCENDIO. EQUIPO PRIMEROS AUXILIOS</i>

4B NIVEL DE RIESGO BAJO

AREA	RIESGO	CONTINGENCIA
PLANTA ALTA		
SALA SESIONES PRESIDENCIA. HABITACIONES. BAÑOS. SALA CONFERENCIAS.	<i>INCENDIO. CORTO CIRCUITO. ATENTADOS. SISMOS</i>	<i>EQUIPO CONTRA INCENDIO/ EQUIPO PRIMEROS AUXILIOS</i>

ACCESOS Y SALIDAS:

ALTERNATIVA#1: PUERTA PRINCIPAL DEL EDIFICIO HACIA LA CALLE G. CORDOVA O HACIA EL PARQUEADERO INTERIOR.

ALTERNATIVA#2: PUERTA LATERAL COCINA HACIA LA CALLE G. CORDOVA O HACIA EL PARQUEO INTERIOR.



OFICINA PRINCIPAL
GUAYAQUIL

PLAN DE RESPUESTA
A CRISIS
P.R.C.

7.- MAPEO DE RIESGOS

SEGURIDAD
SALUD
AMBIENTE

ZONA 5

AREA DE CONCENTRACION

- OPCION # 1 AREA SOLAR DEL FRENTE ESQUINA G.
CORDOVA Y P. SOLANO.
- OPCION # 2 AREA DE PARQUEADERO EXTERNO.
- OPCION # 3 AREA PARQUEADERO INTERNO.

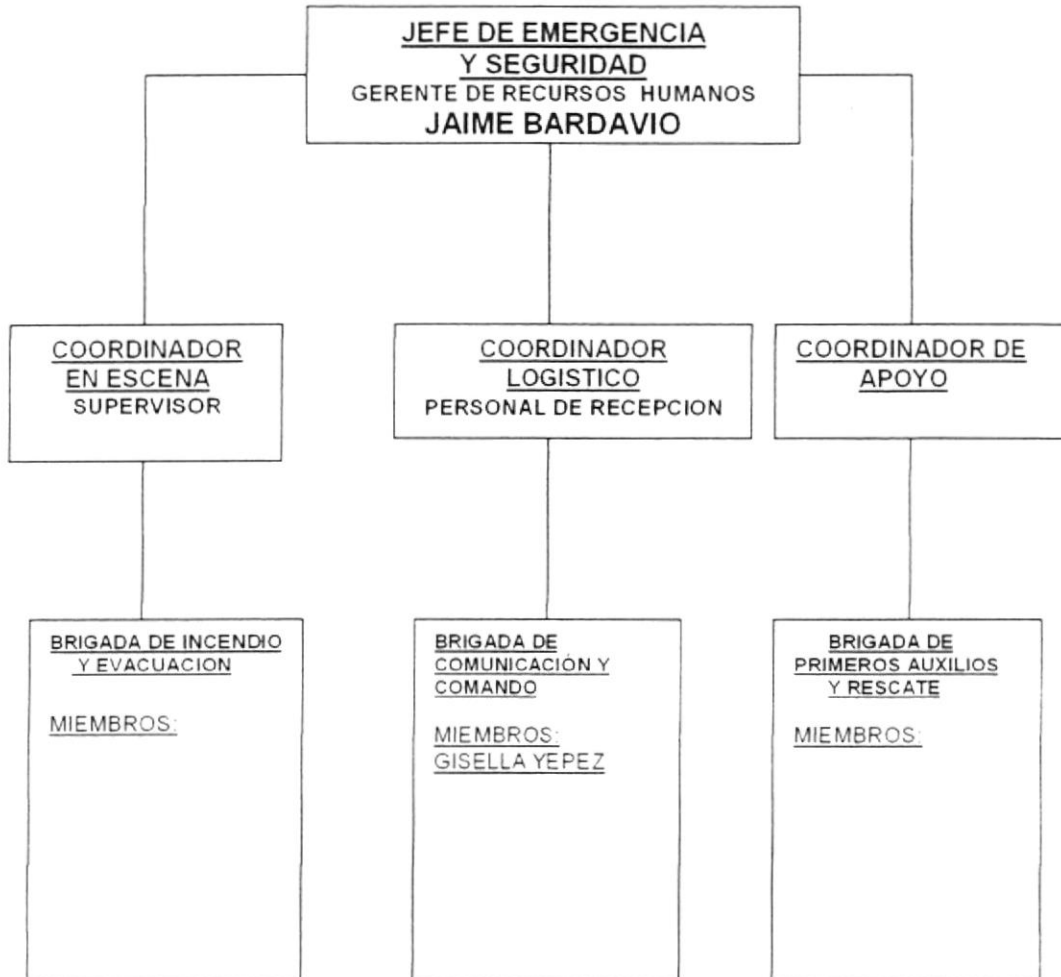


OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C**

8.- ORGANIZACIÓN DE
BRIGADAS

**SEGURIDAD
SALUD
AMBIENTE**





OFICINA PRINCIPAL
GUAYAQUIL

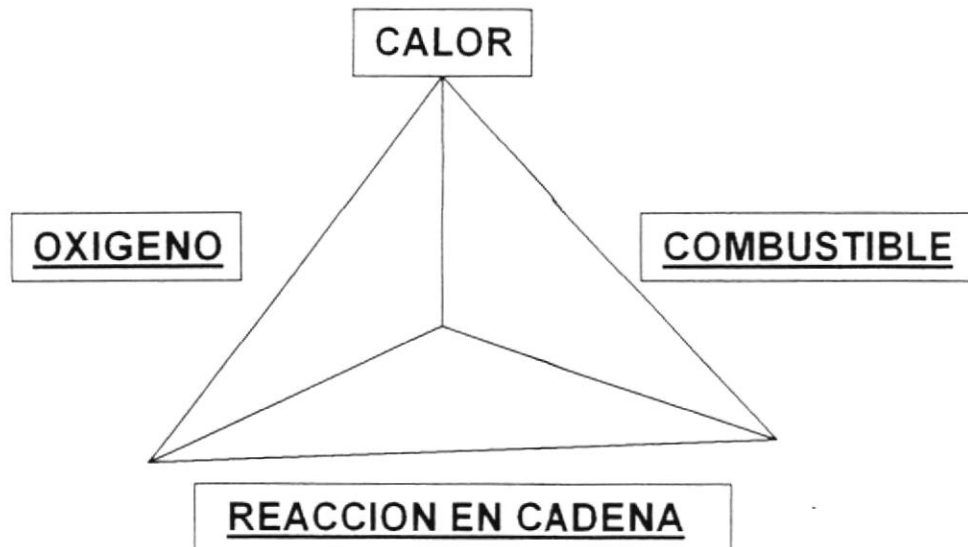
**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

9.- BRIGADA DE INCENDIO Y
EVACUACION

**SEGURIDAD
SALUD
AMBIENTE**

TETRAEDRO DEL FUEGO

LA UNION DE LOS 4 COMPONENTES DEL FUEGO, EN LAS PROPORCIONES NECESARIAS, CONFORMAN EL LLAMADO TETRAEDRO DEL FUEGO.



CAUSAS PRINCIPALES DE INCENDIO

- Dejar equipos encendidos (cafeteras, computadoras, luces, etc.).
- Almacenamiento y manipulación de sustancias químicas sin las debidas condiciones de seguridad.
- Falta de mantenimiento preventivo y correctivo a los equipos, Cortocircuito.
- Deterioro de las instalaciones eléctricas.
- Instalaciones eléctricas improvisadas.
- Electricidad estática.
- Chispas de origen eléctrico, soldadura, etc.
- Fricción mecánica.
- Combustión espontánea.
- Explosión.
- Fumar en las oficinas y colillas encendidas.
- Mala disposición y acumulación de basura.
- Mantener en las oficinas materiales combustibles.



OFICINA PRINCIPAL
GUAYAQUIL

PLAN DE RESPUESTA
A CRISIS
P.R.C.

9.- BRIGADA DE INCENDIO Y
EVACUACION

SEGURIDAD
SALUD
AMBIENTE

Recibida la alarma de emergencia, el personal de la Brigada se constituirá con urgencia en el lugar asignado.

Evaluarán la situación, la cual si es crítica, el Coordinador informará al Jefe del Plan que se proceda a la evacuación del personal.

Adoptará las medidas de ataque que considere conveniente al momento.

Se tomarán los recaudos necesarios sobre la utilización de los equipos de Protección Personal para los integrantes de la Brigada.

Al arribo del Cuerpo de Bomberos, informará de las medidas adoptadas y las tareas que se están realizando, entregando el mando a los mismos y ofreciendo la colaboración de ser necesario.

PROCEDIMIENTOS DE EVACUACION:

Todo el personal deberá conocer las directivas generales del Plan de Evacuación, para lo cual se tomarán los recaudos necesarios para la información permanente, especialmente de los nuevos ingresos a la Empresa. El personal que observe una situación anómala en el área donde se desarrollan sus labores, deberá dar aviso urgente de la siguiente manera:

- ✓ AVISAR AL JEFE INMEDIATO.
- ✓ SE ACONSEJA AL PERSONAL QUE GUARDE LOS VALORES Y DOCUMENTOS, COMO ASI TAMBIEN DESCONECTAR LOS ARTEFACTOS ELECTRICOS A SU CARGO, CERRANDO PUERTAS Y VENTANAS A SU PASO.
- ✓ PROCEDERA A ABANDONAR EL LUGAR SIGUIENDO LAS INSTRUCCIONES DEL COORDINADOR DE EVACUACION.
- ✓ NO PERDER TIEMPO RECOGIENDO OTROS OBJETOS PERSONALES.
- ✓ CAMINAR HACIA LA SALIDA ASIGNADA.
- ✓ CAMINE, NO CORRA, SIN HABLAR, SIN GRITAR, RESPIRANDO POR LA NARIZ.

PROCEDIMIENTO DURANTE EL INCENDIO

- ✓ Inicie la búsqueda y rescate de posibles víctimas y atiéndalas.
- ✓ Controlar, combatir y extinguir un conato de fuego que se presente en las instalaciones.
- ✓ Garantizar la seguridad en las rutas de Evacuación, para que no ofrezcan peligro y facilitando de esta manera, el desalojo oportuno de los ocupantes.
- ✓ Cuando se presente el apoyo del Cuerpo de Bomberos, ordenadamente deben abandonar la zona con los equipos de extinción utilizados y dirigirse al sitio de reunión, permaneciendo en alerta para prestar apoyo y orientación cuando se los requiera.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

9.- BRIGADA DE INCENDIO Y
EVACUACION

**SEGURIDAD
SALUD
AMBIENTE**

EXPLOSION

- ✓ Una vez producida la explosión se deberá hacer una evacuación total de tipo temporal, iniciando por el lugar de la explosión y sus áreas adyacentes, mientras se hace revisión para verificar su estado, los daños y existencia de otros peligros. Para esto deben apoyarse en todos los coordinadores de evacuación, empleados, colaboradores y guías de las diferentes áreas presentes en esos momentos.
- ✓ Verifique lo sucedido e informe inmediatamente al Jefe del Plan de Emergencia.
- ✓ Aléjese del sitio inmediatamente.
- ✓ No se asome por ventanas, ni puertas.
- ✓ Ayude a otras personas de la zona, para que no se acerquen al sitio de la explosión.
- ✓ Si encuentra personas heridas, trate de ayudarlos y retirarlos, avise inmediatamente al Jefe del Plan de Emergencia.
- ✓ Evalúe las condiciones de salida y salga con las personas que están con usted.



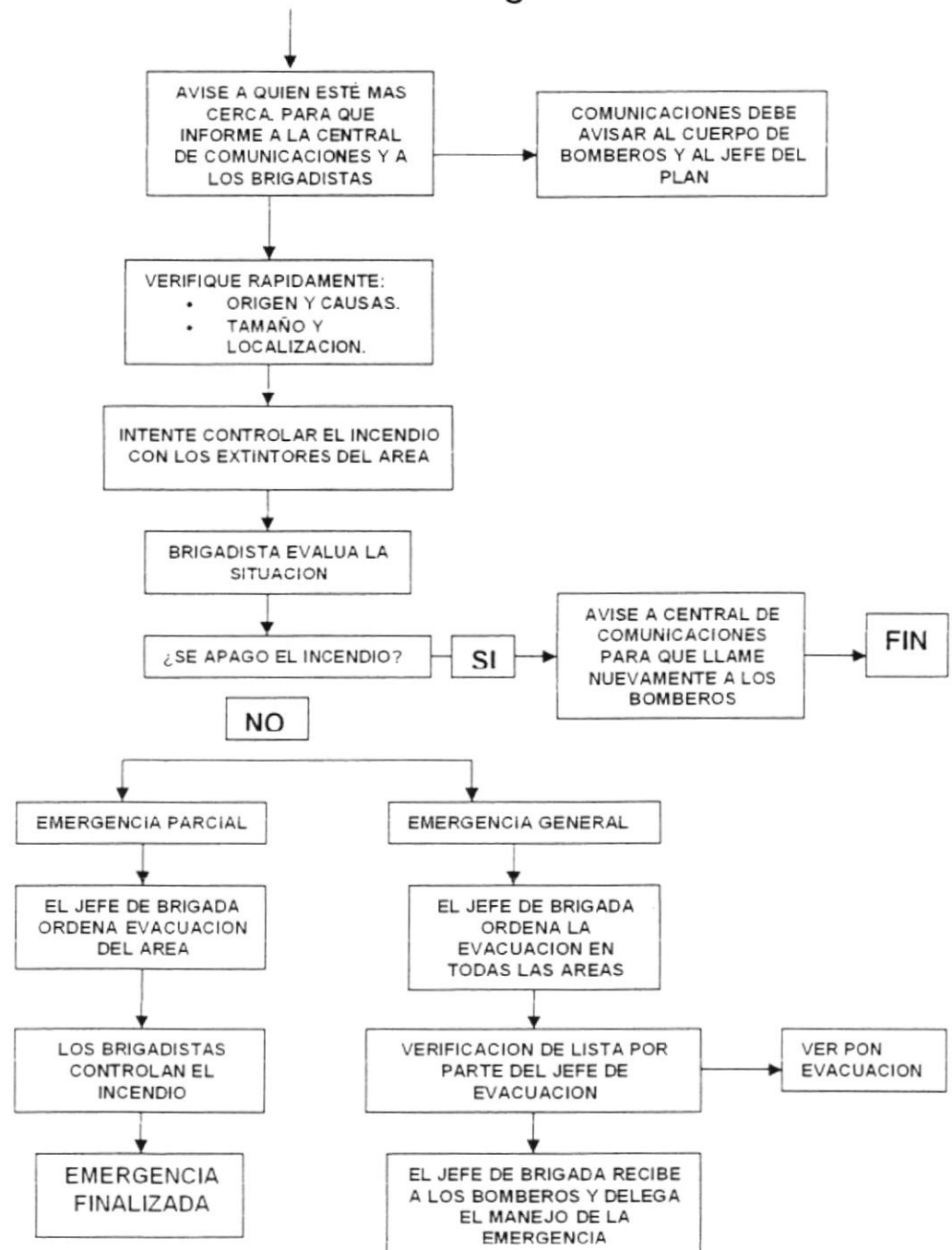
OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

9.- BRIGADA DE INCENDIO Y
EVACUACION

**SEGURIDAD
SALUD
AMBIENTE**

Quien descubra el fuego



 OFICINA PRINCIPAL GUAYAQUIL	PLAN DE RESPUESTA A CRISIS P.R.C.	SEGURIDAD SALUD AMBIENTE
	10.- BRIGADA DE COMUNICACIÓN Y CONTROL	

EQUIPOS Y RECURSOS DEL CENTRO DE COMUNICACIÓN Y CONTROL.

- LINEAS TELEFONICAS # 2560400.
- CELULARES #|
- LINEA SATELITAL.
- RADIO
- COMPUTADORAS
- CORREO ELECTRONICO.
- PLANO DE LAS INSTALACIONES.
- DOCUMENTOS SUGERIDOS.

La respuesta local (Jefe del Plan de Emergencia) se activa simultáneamente con el aviso a la "Central de Comunicaciones" (Conmutador Telefónico o Sala de Radio); su fin debe ser el control de una situación incipiente evitando al máximo el pánico entre los ocupantes, y si se requiere, la solicitud de apoyo especializado.

Luego de la confirmación de la emergencia, se define la gravedad de la misma para definir y activar oportuna y coordinadamente la evacuación de las instalaciones, asegurándose de que se realice con el mínimo de riesgos. La respuesta Externa se activa cuando la emergencia no ha podido controlarse por la organización de la Empresa. Involucra todos los recursos disponibles interna y externamente, y su principal objetivo es lograr el control de la situación con el mínimo de efectos sobre las personas, las vecindades y la imagen de la Empresa.

ACCIONES ANTES DE UNA EMERGENCIA

- Elaborar inventarios de los recursos humanos, físicos y de materiales con que cuenta la Empresa para afrontar emergencias.
- Mantener actualizados los diferentes manuales, mapas de riesgo y rutas de evacuación.
- Velar por el buen mantenimiento de los diferentes recursos materiales y físicos de la Empresa.
- Mantener actualizados los listados del personal, pertenecientes a los diferentes grupos de apoyo.
- Presentar cotizaciones debidamente sustentadas para la consecución de recursos necesarios.
- Organizar archivos con la información necesaria para el control de emergencias.
- Dotar a las Brigadas con los elementos necesarios para garantizar su buen funcionamiento.
- Coordinar y Evaluar las acciones de cada una de las Brigadas.
- Establecer relación permanente con los máximos Ejecutivos de la Empresa.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

10.- BRIGADA DE
COMUNICACIÓN Y
CONTROL

**SEGURIDAD
SALUD
AMBIENTE**

- Distribuir las diferentes responsabilidades a los integrantes de las Brigadas.
- Citar a reuniones periódicas a los miembros de las Brigadas sobre las diferentes acciones que contempla el Plan de Contingencias.

ACCIONES DURANTE UNA EMERGENCIA

- ❖ Activar la cadena de llamadas a los miembros de las Brigadas.
- ❖ Suministrar al Comité de Emergencias y a los grupos de apoyo la información necesaria para el control eficaz de la emergencia.
- ❖ Coordinar el suministro oportuno de los recursos necesarios para afrontar la emergencia.
- ❖ Determinar las necesidades de recursos de cada uno de los grupos de apoyo.
- ❖ Recoger toda la información relacionada con la Emergencia.
- ❖ Realizar contactos con las instituciones de ayuda externa.
- ❖ Facilitar la consecución de recursos no existentes en la Empresa al momento de la Emergencia.
- ❖ Coordinar y ejecutar el control de mando.

ACCIONES DESPUES DE UNA EMERGENCIA

- Coordinar la recuperación de los recursos utilizados.
- Realizar el inventario de recursos para determinar cuáles se deben reponer.
- Determinar las necesidades de nuevos recursos para afrontar futuras emergencias.
- Seleccionar información importante de la emergencia y archivarla.
- Realizar reuniones de evaluación de los procedimientos realizados en la emergencia.
- Recoger el informe de cada una de las Brigadas.
- Presentar el informe respectivo a la Gerencia.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

11.- BRIGADA DE PRIMEROS
AUXILIOS Y RESCATE

**SEGURIDAD
SALUD
AMBIENTE**

PRIMEROS AUXILIOS

Es la ayuda inmediata, necesaria y adecuada que se da a una víctima cuando ha sufrido un accidente o enfermedad repentina hasta llevarla a una casa especializada, sin provocarle más daño del que tiene.

OBJETIVOS :

- Conservar la vida.
- Evitar complicaciones físicas y psicológicas.
- Ayudar a la recuperación.
- Asegurar el traslado de los accidentados.
- Localizar, acceder, estabilizar y movilizar inicialmente a las víctimas, hasta ubicarlas en un sitio de atención seguro.

PRINCIPIOS DE ACCION DE EMERGENCIA

- BIOSEGURIDAD
- EVALUACION DE LA ESCENA.
- ESTADO DE CONCIENCIA DEL PACIENTE.

RECURSOS

- Iluminación.
- Elementos de protección personal.
- Herramientas.
- Botiquines.
- Vehículos.

BOTIQUIN DE PRIMEROS AUXILIOS

El Botiquín consta de solo elementos para los Primeros Auxilios.

No agregar elementos no sugeridos en el botiquín.

Toda medicación adicional debe ser otorgada por un profesional, NO a la automedicación.

LISTADO DE MATERIALES

- Guantes quirúrgicos.
- Máscara y/o equipo de Resucitación Cardio - Pulmonar.
- Gasas estériles.
- Esparadrapo.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

11.- BRIGADA DE PRIMEROS
AUXILIOS Y RESCATE

**SEGURIDAD
SALUD
AMBIENTE**

- Curitas.
- Soluciones antisépticas.
- Linterna.
- Tijera. IJERA.
- Cloruro de sodio 0.9% (solución isotónica).
- Baja lenguas.
- Algodón torundas.
- Jeringuillas descartables.
- Povidin solución jabonosa.
- Povidin solución antiséptica.
- Vendas elásticas.
- Material para férulas.
- Equipo de protección personal: gafas, delantal, guantes, botas.
- Carbón activado.
- Sulfato de magnesio.
- Tierra de Fuller.
- Sulfato de Atropina ampollas.
- Sonda nasogástrica.
- Bolsa roja para material contaminado.
- Bolsa amarilla para ropa sucia.

RIESGOS ASOCIADOS

Físicos.

- Fallas estructurales.
- Fallas eléctricas.
- Explosiones.
- Ahogamiento.

Químicos

- Intoxicación.
- asfixia.

Biológicos

- Contacto con fluidos corporales.(Ver normas de Bioseguridad)

CARACTERISTICAS DEL CONTROL DE ESTABILIZACION Y CLASIFICACION DE LESIONADOS .

OBJETIVO

Recibir, clasificar y estabilizar las víctimas para posterior remisión y transporte hasta un centro de atención hospitalaria especializado.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

11.- BRIGADA DE PRIMEROS
AUXILIOS Y RESCATE

**SEGURIDAD
SALUD
AMBIENTE**

RECURSOS

- ✓ Equipos de protección médico quirúrgica.
- ✓ Asistencia y estabilización.
- ✓ Comunicaciones.
- ✓ Transporte.
- ✓ Iluminación.
- ✓ Carpa.
- ✓ Papelería.
- ✓ Localizar, acceder, estabilizar y movilizar inicialmente a las víctimas, hasta ubicarlas en un sitio de atención seguro.

ATENCIÓN PRE-HOSPITALARIA (APH)

Ubique la mejor área para el Control de Estabilización y Clasificación de lesionados:

- Parqueo de ambulancias
- Seguridad
- Camillas y camilleros.

Calcule el número potencial de víctimas:

- Hora de la Emergencia.
- Ubicación.
- Tipo de instalaciones.

Ubique al personal necesario:

- En el sitio.
- Activar otros hospitales.

Asigne responsables y funciones específicas:

- Asistencia pre-hospitalaria.
- Coordinar el transporte.
- Censo de heridos.

Establezca comunicación con otros Hospitales para remisión:

- Atención hospitalaria.
- Emergencia.
- Referencia Inter.-hospitalaria.

RECUERDE:

- ¿Es seguro realizar el Rescate?
- Delege el manejo de la Emergencia.
- Delimite las zonas de búsqueda.
- Asigne personal por cada área.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

11.- BRIGADA DE PRIMEROS
AUXILIOS Y RESCATE

**SEGURIDAD
SALUD
AMBIENTE**

- Marque las áreas donde ya se realizó la búsqueda.
- Ubique víctimas utilizando los medios de acceso.
- Aplicar los Primeros Auxilios de acuerdo a las lesiones de la víctima.
- Si la víctima no se la puede movilizar, estabilícela en el sitio mismo.
- Si la víctima se puede movilizar, llévela al área de Control de estabilización y clasificación de lesionados.
- Estabilice a las víctimas y priorice el traslado.
- ¿Fueron atendidas todas las personas?

EVALUACION DE LA VICTIMA

Proceso ordenado y sistémico para descubrir lesiones o problemas médicos que si no se tratan, pueden amenazar la vida de un paciente a largo plazo.

- ENTREVISTA
- CONTROL DE SIGNOS VITALES
- REVISION CABEZA A PIES.

- SITUESE CERCA DEL PACIENTE
- INTENTE DAR SEGURIDAD AL PACIENTE, QUE VA HACER ATENDIDO.
- PREGUNTE EL NOMBRE AL PACIENTE.
- PREGUNTE LA EDAD AL PACIENTE.
- DE SER POSIBLE, PREGUNTE, EL DIA Y EL AÑO.
- AVERIGUE QUE DOLENCIA AQUEJA PRINCIPALMENTE AL PACIENTE.
- INTENTE CONOCER LAS CIRCUNSTANCIAS DE LO SUCEDIDO AL PACIENTE.
- DETERMINE LAS CONDICIONES DE SALUD HABITUALES AL PACIENTE.
- PREGUNTE QUE MEDICAMENTOS TOMA REGULARMENTE.
- DETERMINE CUALQUIER TIPO DE ALERGIA QUE SUFRA.

RIESGOS ASOCIADOS

Físicos.

Golpes.
Traumas.
Ergonómicos.

Biológicos

Contacto con fluidos corporales:

NORMAS DE BIOSEGURIDAD

Por el contacto de la sangre con la piel lastimada o con la mucosa de la boca, nariz u ojos puede, potencialmente exponerse al riesgo de contraer enfermedades como HEPATITIS, SIDA; siempre y cuando la persona lesionada esté contagiada.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

11.- BRIGADA DE PRIMEROS
AUXILIOS Y RESCATE

**SEGURIDAD
SALUD
AMBIENTE**

POR ELLO.....CUANDO AUXILIE A ALGUNA PERSONA QUE PRESENTA UN SANGRADO:

- Use guantes descartables y anteojos de seguridad.
- Si debe realizar respiración Boca-Boca use la máscara plástica para cubrir la boca del paciente.
- Lávese muy bien las manos con agua y jabón después de la atención.
- Descarte los guantes, gasas o material que se haya contaminado en la bolsa roja.
- Si hay ropa manchada de sangre, vómitos se deberá colocar en la bolsa amarilla.
- En ambos casos las bolsas debidamente cerradas deben ser trasladadas a salud ocupacional para su disposición final.
- Si hay superficies manchadas con sangre, vómitos u otros fluidos corporales se deberán lavar con una solución clorada (dejar actuar no menos de 20 minutos); cuando lo haga colóquese guantes y si es necesario botas de caucho.
- Todos los materiales utilizados serán renovados según necesidad.

En el caso de encontrar elementos punzantes que pudieron estar en contacto con sangre (jeringuillas, agujas, vidrios, etc.) deberá colocarse los guantes y disponer estos elementos dentro de un recipiente rígido: botella de plástico, caja de cartón, etc. para luego colocarlo en la bolsa roja y trasladarlo a Salud Ocupacional para su disposición final.

ANTE CUALQUIER DUDA , CONSULTE CON PERSONAL DE SALUD OCUPACIONAL.

Si hubiera existido contacto de la sangre con la piel lastimada, mucosas de nariz, boca u ojos, lávese con abundante agua y jabón, avise o concurra de inmediato a Salud Ocupacional.

RESCATE

BUSQUEDA
LOCALIZACION
ACCESO
ESTABILIZACION
EXTRACCION

FUNCIONES DEL JEFE DE LA BRIGADA

- Coordinar la operación de Rescate, todas las acciones a desarrollar.
- Responsable de la seguridad.
- Cuidado de los equipos, herramientas y accesorios.



OFICINA PRINCIPAL
GUAYAQUIL

PLAN DE RESPUESTA
A CRISIS
P.R.C.

11.- BRIGADA DE PRIMEROS
AUXILIOS Y RESCATE

SEGURIDAD
SALUD
AMBIENTE

- Responsable del egreso e ingreso del personal.
- Controlar el uso del equipo de protección personal.
- Asignar las tareas a los miembros de la Brigada.
- Mantener la rotación del trabajo.
- Decidir que herramienta utilizar de acuerdo a la tarea.
- Fomentar el espíritu de compañerismo en el grupo.

FUNCIONES DE LOS MIEMBROS DE LA BRIGADA

- Recibir las asignaciones del Jefe de la Brigada.
- Cumplir la misión en situaciones de tensión.
- Valorar adecuadamente las situaciones de peligro.
- Será responsable de su propia seguridad.
- Conocimiento de las operaciones de rescate.
- Tomar decisiones rápidas y firmes.
- Habilidad para comunicarse, informará al Jefe de la Brigada del progreso de la tarea.
- Buenas condiciones físicas.
- Habilidad y destreza manual.
- Trabajar en equipo y coordinado.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

12.- ALTERACION DEL
ORDEN PUBLICO

**SEGURIDAD
SALUD
AMBIENTE**

DISTURBIOS CIVILES:

ACCIONES DEL JEFE DEL INCIDENTE:

- ❖ Verificar zona y magnitud de los disturbios con la Policía Nacional local.
- ❖ Notificar de inmediato a oficina central.
- ❖ Notificar a autoridades locales (usar formato de reporte de incidente).

INSTALACIONES AMENAZADAS:

ACCIONES DEL EQUIPO DE MANEJO DE CRISIS:

- a. Definir centro de comando y sistema de comunicación.
- b. Activar planes de protección de la instalación.
- c. Mantener registro de comunicaciones con autoridades. Si las instalaciones están amenazadas deben establecerse parqueos alternos y rutas alternas de suministros y evacuación.


PROCEDIMIENTOS EN AREA DESPACHOS:

INSTRUCCIONES:

- a. Evite despachar vehículos hacia zona de disturbios.
- b. Establezca un programa de notificación de fuerza mayor a clientes.
- c. Notifique a los Gerentes.
- d. Si es indispensable despachar hacia la zona de disturbios, solicite escolta policial.
- e. Verifique rutas alternas de despacho.
- f. Evite las áreas donde haya disturbios civiles.
- g. Avise a su supervisor sobre contactos que tenga entre las autoridades locales.

ACCIONES DE CONDUCTORES QUE ENCUENTREN DISTURBIOS:

- a. Movilizar el vehículo fuera del área inmediatamente.
- b. Solicitar escolta policial para evacuar el área.
- c. Telefonar al supervisor o al centro de despachos para instrucciones adicionales.
- d. Si cree poder hacer la entrega utilizando una ruta alterna, hágalo.
- e. Si no puede terminar de hacer el despacho, regrese a la empresa o aléjese del lugar.
- f. Si no puede movilizar el vehículo, notifique a la policía y bomberos.

 <p>OFICINA PRINCIPAL GUAYAQUIL</p>	<p>PLAN DE RESPUESTA A CRISIS P.R.C.</p> <p>12.- ALTERACION DEL ORDEN PUBLICO</p>	<p>SEGURIDAD SALUD AMBIENTE</p>
--	--	--

- g. No abandone el vehículo excepto bajo órdenes policiales o si su vida está en peligro.
- h. Al bajarse del vehículo bloquéelo y tome las llaves, contacte con su supervisor.

TERRORISMO:

PROCEDIMIENTO GENERAL

Si usted recibe una llamada:

- Conserve la calma, sea cortés y no demuestre miedo. Calmarse es la acción más importante que usted puede realizar en caso de amenaza de bomba.
- Escuche con atención y tome nota de la hora en que recibió la llamada, las palabras exactas de lo que dijo y los detalles durante o inmediatamente después, tales como sexo, acento, actitud, ruidos, motivo.
- Advierta que la Empresa está ocupada con personas y puede ocasionar muertes o heridas serias.
- Mantenga al que llama lo más ocupado posible.
- Si no indica la hora y ubicación del atentado, pregúntele.
- Después de la llamada, notifique. Informe inmediatamente a la Gerencia o a la persona que al momento haga las veces (Cadena de reemplazos).
- No discuta / informe solo a las personas autorizadas.
- Si es correo bomba, no manipule ningún paquete extraño y aléjese inmediatamente.
- No corra, verifique la situación (lugar, tipo de artefacto, afectación, etc.).
- Siempre mantenga informado a la Gerencia o Brigada de Incendio y Evacuación).
- Salga despacio, en dirección contraria a donde está sucediendo el evento.
- Siga las instrucciones del Jefe de la Brigada, ya que no siempre las rutas de evacuación preestablecidas pueden ser las correctas.
- Lleve consigo a todo el personal visitante.
- Verifique y reporte paquetes extraños, cajas u otros materiales que no estén en su sitio.
- No los mueva, no agregue agua, ni otros elementos sobre ellos.
- No permita el uso de aparatos de radio, celulares, ya que la señal electrónica puede activar el artefacto explosivo.

PARA LOS MIEMBROS DE LA BRIGADA

- Reúnase inmediatamente a reunirse con los demás miembros de su Brigada.
- Verifique inmediatamente la situación de los edificios e informe al Jefe de Brigada de Incendio y evacuación.
- Solicite ayuda externa de ser necesario. Consulte el Directorio telefónico anexo al presente documento.
- Ordene inmediatamente que un miembro de la Brigada reciba a los grupos de ayuda (como antiexplosivos) y que coordine las acciones con ellos.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

12.- ALTERACION DEL
ORDEN PUBLICO

**SEGURIDAD
SALUD
AMBIENTE**

- Tome las decisiones necesarias para preparar los servicios de urgencias externos para la recepción de pacientes que han sido afectados por la explosión.
- Verifique el estado de los servicios públicos y de la estructura.
- Verifique si es necesario abandonar áreas y dé la orden de evacuación inmediata, especialmente las áreas cercanas a la bomba.
- Informe periódicamente a la Gerencia.
- Verifique la situación que está sucediendo.
- Realice rondas por las instalaciones si se trata de un artefacto explosivo dentro del edificio, y en conjunto con los empleados detecte cajas o elementos sospechosos. También en la parte externa del edificio si se trata de un carro bomba: realice rastrillo, evalúe y mantenga el control interno.
- Verifique la información de llamadas o de otros trabajadores.
- Informe de la situación a la Gerencia o al Jefe del Plan de Contingencia y coordine para proceder de acuerdo con la situación.

EXPLOSION

PROCEDIMIENTO GENERAL

- ✓ Calmarse, es la acción más importante que usted puede hacer.
- ✓ Infórmese donde ocurrió la explosión.
- ✓ Informe inmediatamente a la Gerencia y al Jefe de Brigada de Incendio y Evacuación.
- ✓ Aléjese de la zona de explosión, no se acerque a ventanas, cúbrase como en el caso de sismo.
- ✓ Ayude a evacuar la zona inmediatamente.
- ✓ Acordone la zona, no permita que nadie se acerque, pueden existir otros riesgos (nuevas explosiones, colapsos de estructuras).
- ✓ Con las personas tenga sumo cuidado, sobre todo con elementos que le puedan caer o hacer daño.
- ✓ Notifique de inmediato a los grupos de socorro, en especial a los bomberos, la Cruz Roja y a la Unidad antiexplosivos.
- ✓ No permita que nadie ingrese.

PARA LOS MIEMBROS DE LAS BRIGADAS

- Reúnase inmediatamente con los demás miembros de su Brigada.
- Verifique inmediatamente la situación de los edificios e informe al Jefe de la Brigada.
- Haga o solicite informes de una evaluación estructural de los edificios, así como de la zona donde ocurrió la explosión, pueden ocurrir colapsos de estructuras.
- Solicite ayuda externa de ser necesario. Consulte el Directorio telefónico anexo al presente documento.
- Ordene inmediatamente que un miembro de las Brigadas reciba a los grupos de ayuda y que coordine las acciones con ellos.



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

12.- ALTERACION DEL
ORDEN PUBLICO

**SEGURIDAD
SALUD
AMBIENTE**

- Tome las decisiones necesarias para preparar los servicios de urgencias para la recepción de pacientes que han sido afectados por el incendio.
- Verifique el estado de los servicios públicos y de la estructura.
- Verifique si es necesario abandonar áreas y dé la orden de evacuación inmediata.
- Ordene de acuerdo a las circunstancias.

AMENAZA DE BOMBA:

ACCIONES A DESARROLLAR:

- a. Notifique inmediatamente al Gerente. Si la amenaza es por escrito, manéjela con discreción y guárdela como evidencia.
- b. Si la amenaza es telefónica, mantenga la persona en la línea tanto como sea posible.
- c. Elabore el formato de amenaza de bomba.

EVALUE LA CREDIBILIDAD DE LA LLAMADA Y TOME LAS SIGUIENTES MEDIDAS:

- a. Evacue de inmediato al personal de la instalación hacia los puntos de reunión.
- b. No permita el ingreso del personal hasta que la instalación sea declarada segura.
- c. Notifique a la policía y otros servicios de emergencia locales.
- d. Seleccione el personal de la Brigada contra Incendio y Evacuación que conozca bien las instalaciones.
- e. Asigne uno o dos acompañantes a los equipos de búsqueda de la policía.
- f. Evacuar el personal desde los puntos de reunión hacia el exterior de la planta.
- g. Si se conjura la emergencia, coordine el ingreso del personal.

PROCEDIMIENTO AMENAZA DE ATENTADO

- ✓ Si ha recibido notificación de la posible existencia de un artefacto explosivo, haga una evaluación preliminar de la información obtenida.
- ✓ Si la posible ubicación del explosivo es conocida, verifique con el personal de seguridad la existencia del explosivo.
- ✓ Si no se conoce la posible ubicación del artefacto explosivo, analice la credibilidad de la amenaza; si existen elementos que generen incertidumbre, evacue y aisle en forma inmediata la edificación.
- ✓ Antes de evacuar, cada empleado o brigadista deberá revisar su área de trabajo para identificar objetos extraños o sospechosos.
- ✓ Notifique a las autoridades de Policía para que ellos realicen una búsqueda y control en el área, hasta que se tenga la certeza de que no existe peligro.




OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

12.- ALTERACION DEL
ORDEN PUBLICO

**SEGURIDAD
SALUD
AMBIENTE**

- ✓ Si se encuentra en las instalaciones un elemento del cual se sospecha que puede ser un artefacto explosivo, evacue y aisle en forma inmediata el área amenazada y notifique a la Policía para que determine la veracidad no de la amenaza.
- ✓ Si la amenaza es real, los expertos antiexplosivos de la Policía o el Ejército harán la desactivación del artefacto; en caso contrario lo retirarán del área y/o lo harán explotar en forma controlada.
- ✓ En caso de ser real la amenaza, se deberá hacer una revisión de todas las demás áreas del Hospital, para establecer si existen otros artefactos explosivos.

 OFICINA PRINCIPAL GUAYAQUIL	PLAN DE RESPUESTA A CRISIS P.R.C.	SEGURIDAD SALUD AMBIENTE
	13.- SISMOS TERREMOTOS	

**PROCEDIMIENTOS GENERALES PARA
PERSONAL DE PLANTA :**


- a. Suspenda la entrega de Producto terminado.
- b. Suspenda el recibo de materiales.
- c. Corte la energía de toda la planta.
- d. Evacue de las áreas de producción, zona de tanques, etc.
- e. Aléjese de las líneas eléctricas aéreas (Si puede, dirijase al punto de reunión).
- f. Aléjese de estanterías y stock.
- g. No retire banqueros sin autorización.
- h. Salga de su puesto de trabajo, siguiendo las rutas de evacuación.
- i. No corra, conserve la calma, no alarme a otros.
- j. No se regrese por ningún motivo.
- k. No retire vehículos sin autorización.

PERSONAL DE OFICINAS:

- a. Abandone su lugar de trabajo por las rutas de Evacuación indicadas.
- b. Ubíquese en los puntos de reunión.
- c. Conserve la calma y ayude a otros a conservarla.
- d. No se regrese por ningún motivo.
- e. Espere instrucciones para realizar la evacuación general.
- f. No retire vehículos sin autorización.

SISMO

- PROTEJASE ANTE EL SISMO, como cualquier persona lo haría y de acuerdo a las instrucciones generales mencionadas con anterioridad.
- SI VE SITUACIONES FUERA DE LO NORMAL, comuníquese con el Brigadista de su área o con el que usted vea primero e infórmele.
- COMIENCE LA EVACUACIÓN, de acuerdo a las indicaciones de los Brigadistas, no regrese y facilite las labores de los grupos de socorro. Siga las instrucciones de los Brigadistas.
- SALGA ORDENADAMENTE.
- SI VE VISITANTES, llévelos con usted e indíqueles el camino.
- CON LOS HERIDOS, sea muy cuidadoso y no los mueva a menos de que sea estrictamente necesario. Si está UD. con un herido, cálmese y solicite ayuda de los brigadistas y del personal de salud, no lo mueva.

 <p>OFICINA PRINCIPAL GUAYAQUIL</p>	<p>PLAN DE RESPUESTA A CRISIS P.R.C.</p> <p>13.- SISMOS TERREMOTOS</p>	<p>SEGURIDAD SALUD AMBIENTE</p>
--	---	--

Mientras sale del lugar:

- VERIFIQUE el gas, agua y líneas eléctricas y asegúrese si hay alguna avería e informe inmediatamente al jefe de Brigada. Si percibe algún olor a gas cierre la válvula principal. No encienda el gas o utilice la electricidad hasta que la edificación no haya sido inspeccionada. No encienda fósforos mientras investiga algún escape de gas.
- DESCONECTE el sistema de electricidad, si existe alguna avería en las conexiones eléctricas o tendidos del edificio. Tenga mucho cuidado de no desconectar líneas o sectores importantes a menos de que reciba orden de ello.
- NO TOQUE cables que estén en el piso o enseres eléctricos que estén averiados.
- CONTROLE los químicos, gasolina y otros líquidos inflamables que se hayan derramado.
- VERIFIQUE el estado de los cilindros de gas comprimido, así como de otros envases que puedan caer o volcarse.
- VERIFIQUE que las tuberías de los servicios sanitarios estén en buenas condiciones antes de usar los mismos. De ser necesario tapone los desagües de las bañeras y los fregaderos para evitar el retorno de aguas negras.
- VERIFIQUE si han ocurrido daños a la estructura del edificio, especialmente grietas e informe inmediatamente al Jefe de Brigada.
- ESTE PREPARADO para temblores posteriores. Usualmente son menos intensos que el temblor principal pero alguno podría ser suficientemente fuerte como para causar daños adicionales a la estructura ya debilitadas durante el primer temblor.
- NO MUEVA usted solo a las personas heridas a menos que estén en peligro de tener una nueva lesión.
- BUSQUE ayuda con otras personas para movilizarlo, ayude al herido socorriéndolo con los primeros auxilios básicos, cúbralo o arrópelo con mantas, abrigos, sacos o chaquetas, para evitar su enfriamiento. Si lo movilizó, llévelo a sitio seguro (Centro de Estabilización y clasificación de lesionados).
- BUSQUE ayuda médica mientras otras personas acondicionan el lugar y socorren a los demás heridos; si está en posibilidades de evacuarlos hacia un centro médico asistencial hágalo bajo la supervisión médica trasladándolos en camillas, pero recuerde que cualquier traslado bajo condiciones adversas puede agravar o provocar lesiones. Pueden utilizar sillas para trasladar a personas lesionadas, tablas, hamacas, colchones, si es de llevarlos en vehículos trate de conseguir una camioneta pick-up acondicionada para llevar las personas lesionadas.
- REPORTE la ubicación del herido a los Brigadistas. Nunca lo deje solo; siempre debe haber alguien con él para ayudarlo psicológicamente, indíquele a la persona lesionada que ya pidieron ayuda, no le haga



OFICINA PRINCIPAL
GUAYAQUIL

**PLAN DE RESPUESTA
A CRISIS
P.R.C.**

13.- SISMOS
TERREMOTOS

**SEGURIDAD
SALUD
AMBIENTE**

referencias de las heridas que tiene, manténgalo distraído hablándole de cosas varias, si es posible rece junto a él.

- SIEMPRE establezca comunicación directa con su Jefe de Brigada e informe toda situación anormal que se presente.

TERREMOTO

- Mantenga la calma. Durante un terremoto usted puede experimentar un temblor que empieza suavemente y en cuestión de uno o dos segundos crece tan violentamente que lo puede tirar al piso o sacudirlo con una vibración violenta.
- No salga durante el sismo. No por que no quiera, sino por qué simplemente no va a poder, el piso se está moviendo y están cayendo objetos y cosas.
- Protéjase. Invite, dando ejemplo, a calmarse y a buscar refugio bajo una mesa o mueble fuerte, JAMAS BAJO EL MARCO DE UNA PUERTA (es una costumbre que hace mucho salvó vidas, hoy las está acabando), manténgase lejos de ventanas y objetos que pueden caer, apilamientos de mercancías, estantes, Exhibiciones, bibliotecas, cuadros, etc.
- Evalúe luego del sismo indicios de daño en la estructura (paredes, techos, columnas etc.); evalúe la ruta de salida y salga o busque una salida alterna.
- Salve la información. Si está trabajando en un computador trate de salvar la información y apagar el equipo, es importante, pero no dude en que es primero su vida.
- Salga despacio. No se apresure, no hable, manténgase en silencio.
- No se ubique debajo de cornisas, balcones, o aleros, pueden estar mal contruidos y caerse.
- En corredores o pasillos, arrodílese junto a una pared interior lejos de las ventanas y elementos que puedan caer. Coloque su cabeza cerca a las rodillas, cúbrala con los codos y junte las manos fuertemente detrás de la nuca.
- Revise muy bien las instalaciones. Verifique debajo de muebles, baños y armarios que no queda gente al interior de la edificación. Bloquee la entrada al área afectada, utilice para ello una silla volteada a la entrada, trancando la puerta o señale muy bien la zona con letreros "nadie en la zona".
- No regrese por ningún motivo. Las instalaciones pueden no ser muy seguras o puede ocurrir una réplica del sismo principal y hacer caer más instalaciones.
- No use los teléfonos, a menos que haya una herida seria. Para procedimientos de emergencia más detallados consulte su libro de primeros auxilios.
- Absténgase de curiosear por las calles, no toque cables eléctricos caídos, ni tampoco objetos que estén en contacto con esas líneas de conducción de energía, no prenda luces o linternas, puede haber gases acumulados y producir una explosión.



OFICINA PRINCIPAL
GUAYAQUIL

PLAN DE RESPUESTA
A CRISIS
P.R.C.

13.- SISMOS
TERREMOTOS

SEGURIDAD
SALUD
AMBIENTE

- Dirijáse inmediatamente a la zona de concentración, si no es factible manténgase en el lugar más seguro que al momento encuentre, espere instrucciones adicionales.

 <p>OFICINA PRINCIPAL GUAYAQUIL</p>	<p>PLAN DE RESPUESTA A CRISIS P.R.C.</p> <p>14.- PROCEDIMIENTOS- RELACIONES PUBLICAS</p>	<p>SEGURIDAD SALUD AMBIENTE</p>
--	---	--

COORDINADOR DE INFORMACION Y PRENSA

Debe ser alguien de los niveles directivos de la Empresa (Jefe del Plan de Contingencias).

ANTES

- Acordar con el Jefe del Plan de Contingencias que tipo de información y en que forma debe divulgarse en caso de emergencia.
- Definir el sitio exacto donde se realizarán las ruedas de prensa para informar a los medios de comunicación en caso de una emergencia o incidente que involucre la imagen o responsabilidad de la Empresa.
- Mantenerse actualizado sobre criterios, técnicas y procedimientos de comunicación efectiva en caso de emergencia de acuerdo con las políticas de la Empresa.

DURANTE

- Preparar junto con el Jefe de Emergencia los "comunicados oficiales" en caso de que se requieran.
- Servir de "portavoz" oficial de la Empresa ante la comunidad y los medios de comunicación.
- Divulgar los comunicados oficiales en los diferentes medios y coordinar actividades como "ruedas de prensa" si es necesario.
- Coordinar la atención de los diferentes medios de comunicación con todos los servicios.

DESPUES

Coordinar con el Jefe de Emergencia las actividades de relaciones públicas posteriores al siniestro que faciliten la recuperación de la imagen de la Empresa. Especialmente si la situación ha implicado efectos adversos a terceros o a la comunidad.

Llevar un archivo de toda la información referente al siniestro publicada en los diferentes medios de comunicación.



OFICINA PRINCIPAL
GUAYAQUIL

PLAN DERESPUESTA
A CRISIS
P.R.C.

15.-TELEFONOS DE
EMERGENCIA

SEGURIDAD
SALUD
AMBIENTE

DEFENSA CIVIL

911
2421025
2421020

CUERPO DE BOMBEROS

911
102

CRUZ ROJA

911
2560674
2560675
2561628

COMISION DE TRANSITO

911
103

POLICIA NACIONAL

101

HOSPITALES:

LUIS VERNAZA

2560300
2562171

GUAYAQUIL

2843487
2844587

TERRITORIAL

2282801
2282802


SEGURO SOCIAL

2490666

SOLCA

2288088

REGLAMENTO DE SEGURIDAD,
HIGIENE Y SALUD DE LOS
TRABAJADORES y
MEJORAMIENTO DEL MEDIO
AMBIENTE DE TRABAJO DE LA
CIA. **AGRIPAC S.A.**



**REGLAMENTO DE SEGURIDAD, HIGIENE Y SALUD DE LOS TRABAJADORES Y
MEJORAMIENTO DEL MEDIO AMBIENTE DE TRABAJO.
DE LA COMPAÑÍA AGRIPAC S. A.**


La Compañía **AGRIPAC S. A.**, con la finalidad de precautelar la integridad de sus trabajadores y la del personal que directa o indirectamente labora en sus instalaciones o fuera de ella cuando ostente representación de **AGRIPAC S. A.**, y defender el patrimonio material de la Compañía en cumplimiento con lo dispuesto en el artículo 441 del Código de Trabajo vigente, y con lo establecido en el Decreto Ejecutivo No. 2393 publicado en el Registro Oficial No. 565 del 17 de Noviembre de 1986, que dispone la obligatoriedad del empleador de elaborar y someter a la aprobación del Ministerio de Trabajo, por medio de la Dirección de Trabajo del Litoral, un Reglamento de Seguridad y Salud de los trabajadores y mejoramiento del Medio Ambiente de trabajo y en ejercicio de sus funciones legales resuelve:

Dictar el presente Reglamento de Seguridad y Salud de los trabajadores y mejoramiento del Medio Ambiente de trabajo que será parte integral del Reglamento Interno de la Compañía **AGRIPAC S. A.**, y de conformidad con las disposiciones constantes en lo siguiente artículos:

CAPITULO I

DISPOSICIONES GENERALES

Art. 1.- La compañía **AGRIPAC S. A.**, establecida de acuerdo con las Leyes del Estado Ecuatoriano, con su edificio matriz ubicada en las calles General Córdova No. 623 y Padre Soiano de esta ciudad de Guayaquil, considerando riesgos de accidentes y en cumplimiento de lo previsto en el Artículo No. 441 y siguientes del Código de Trabajo, emite el presente reglamento, con el objeto de:

1. Garantizar condiciones seguras a su personal en todo lugar que éstos desarrollen sus actividades.-
2. Salvaguardar la vida, salud e integridad física de los empleados y terceras personas mediante la eliminación o reducción de las causas de accidentes -  |

CAPITULO II



POLÍTICA, DEFINICIONES Y PROCEDIMIENTOS DE SEGURIDAD TOTAL

Art. 7.- La Compañía **AGRIPAC S. A.**, Establece que todo sistema o proceso de trabajo se realice dentro de las mejores condiciones de Seguridad Total de tal manera que al desarrollarse cualquier operación se considere primordialmente la protección de su elemento humano. También considera de vital importancia la aplicación de las medidas de Seguridad Total, por lo que estimulará y apoyará las iniciativas y sugerencias que se formulen para la prevención y control de los riesgos en general hacia el interior y exterior de la compañía, incluyendo terceras personas con énfasis en la protección del cliente externo, dentro de un marco de Control Total de Perdidas.-

Art. 8.- Cuando en este reglamento se mencione la palabra "**Seguridad Total**" se entenderá que son las normas y medidas de Seguridad Integral, Salud Ocupacional y Seguridad ambiental llamadas simplemente Seguridad, Salud y Ambiente, y destinadas a prevenir accidentes con efectos en el hombre, recursos materiales, bienes e intereses de la compañía.-

Art. 9.- El marco de la Seguridad Total incluye a la Seguridad e Higiene del Trabajo, disciplina aceptada como la tradicional, considerando el aspecto legal ecuatoriano.-

Art. 10.- Accidente de trabajo es todo suceso imprevisto y repentino que ocasiona al trabajador una lesión corporal o perturbación funcional que produce incapacidad temporal, permanente parcial o total y hasta la misma muerte, y que resulta con ocasión o por consecuencia del trabajo que ejecuta por cuenta ajena.-

Art. 11.- También se entenderán por accidente, toda interrupción anormal de un proceso.-

Art. 12.- Incidente es todo suceso imprevisto y repentino, el mismo que con una ligera modificación del sistema, pueden transformarse en accidentes de trabajo.-

A handwritten signature in black ink, located at the bottom right of the page, overlapping the end of the text in Article 12.



compañeros de trabajo harán conocer al supervisor de lo acontecido, a fin de que arbitren las medidas que se requieran.-

Art. 22.- Cuando ocurra un accidente, el accidentado deberá ser trasladado al Hospital del Instituto Ecuatoriano de Seguridad Social, de conformidad con las políticas, normas y procedimientos de Seguridad en el Trabajo, determinados por la compañía.-

Art. 23.- Es obligación de todo Supervisor o Jefe, analizar e investigar el accidente, para proceder luego a enviar un reporte al departamento de Seguridad Total y Recursos Humanos en un lapso no mayor a 48 horas de haberse producido el mismo.-

Art. 24.- La empresa no es responsable por ningún accidente que haya sido provocado deliberadamente o por culpa grave de la víctima, así como también no será responsable si se agravan las lesiones o perturbaciones por razón de haberlo demorado sin justa causa.-

Art. 25.- Cualquier falsedad o engaño por parte del trabajador al suministrar los datos para el reporte de accidente, será considerado como falta grave para la compañía, y será causal de Visto Bueno.-

CAPITULO III

ORGANIZACIÓN DE SEGURIDAD TOTAL

Art. 26.- La Compañía AGRIPAC S. A., con el objeto de prevenir todo tipo de accidentes en general, que pudieren afectar a sus Recursos Humanos, Técnicos y Materiales mantienen estratégicamente la siguiente cobertura:

SEGURIDAD TOTAL COMPRENDE.- La Seguridad Integral, Salud Ocupacional y Seguridad Ambiental

SEGURIDAD INTEGRAL.-

1. Prevención de lesiones
2. Control de daño a la propiedad

and 1



5. Llevar y hacer conocer a todo el personal con mando la estadísticas de accidentes en general, tanto de Recursos Humanos y Servicios como de daño de la propiedad.-
6. Coordinar efectivamente con la estructura organizacional de la Compañía **AGRIPAC S. A.**, a fin de que se cumplan las políticas, normas y procedimientos de Seguridad Integral, Salud Ocupacional y Seguridad Ambiental.-
7. Brindar un asesoramiento y coordinación efectiva para que se cumpla los objetivos de Seguridad Control Incendios y Emergencias de la Compañía.-

Art. 28.- El Departamento de Seguridad Total de la Compañía **AGRIPAC S. A.**, esta ubicado bajo la dependencia del área de Recursos Humanos.-

Art. 29.- La compañía **AGRIPAC S. A.**, acepta su responsabilidad según lo dispuesto por las leyes del Ecuador tales como:

El Registro Oficial No. 565 de 17 de Noviembre de 1986, Decreto No. 2393 sobre Reglamento de Seguridad y Salud de los Trabajadores y mejoramiento del medio Ambiente de Trabajo Titulo 1, Artículo 14.-

El Reglamento de Seguridad e Higiene del Trabajo del Instituto Ecuatoriano de Seguridad Social, Resolución No. 172 Titulo IV, Capitulo I Artículo 116.-

Por lo que crea el Comité de Seguridad y Ambiente como máxima autoridad para determinar las políticas, normas y procedimientos de prevención de accidentes, de enfermedades ocupacionales y protección ambiental.-

Art. 30.- El comité de Seguridad de la Compañía **AGRIPAC S. A.**, estará integrado por tres representantes del empleador y tres representantes de los trabajadores quienes tendrán voz y voto. Se nombrara un Presidente y un Secretario. Cada miembro deberá designar un Suplente quien lo representará en las reuniones a las cuales no puedan asistir, estos suplentes deberán ser nombrados en una reunión del Comité de Seguridad. Todos los miembros ejercerán sus funciones durante un año pudiendo ser reelegidos.-

Art. 31.- El Comité de Seguridad total de la Compañía **AGRIPAC S. A.**, tendrá las siguientes funciones: *PL*

Art. 34.- Todos los empleados de la compañía **AGRIPAC S. A.**, y trabajadores Tercerizados deberán tener uniforme y ropa adecuada para el clima donde realiza sus actividades, de tal forma que siempre se considere con mayor prioridad la protección de la salud y la vida.-

Art. 35.- Todos los trabajadores en general que estén expuestos a riesgos que atenten a su integridad, usarán los elementos de protección personal apropiados como: respiradores, cinturones de seguridad, botas de seguridad, guantes, etc.-

Art. 36.- Todas las instalaciones, permanentes o temporales, deben ser de construcción adecuada para evitar riesgos de accidentes en general.-

Art. 37.- Cuando se desee construir una estructura o instalación, se tendrá en cuenta el ornato y distribución del edificio, de tal manera que no obstaculice algún proceso o actividad, debiendo ser construido o ampliado con miras al futuro.-

Art. 38.- Todo el edificio debe mantenerse libre de obstáculo, basura maleza en sus alrededores.-

Art. 39.- Las vías internas, pasillos áreas y espacios de circulación deben estar libres de obstáculos a no ser que el proceso lo requiera temporalmente y considerándose las normas de seguridad.-

Art. 40.- En las vías internas, estructuras metálicas, pasillos, descansos, etc. debe evitarse el hacinamiento anormal, sea este humano, mecánico, materiales, etc.-

Art. 41.- Es obligación de todos los trabajadores mantener el sitio de trabajo limpio, las zonas de tránsito libre de obstáculos y las áreas alrededor de los equipos contra incendio despejados.-

Art. 42.- En las plantas, bodegas, oficinas, talleres u otros lugares donde existen máquinas individuales y unidas en serie, se debe dejar suficiente espacio alrededor de las



Art. 51.- Todos los interruptores y de más sistemas de control, deberán tener siempre sus cajas apropiadas.-

Art. 52.- Todos los conductores, maquinarias y equipos eléctricos en general, deberán mantenerse dentro de sus niveles de aislamiento y capacidad térmica nominal.-

Art. 53.- En general, todas las maquinarias, equipos y herramientas eléctricas deben tener conexión a tierra.-

Art. 54.- Los cercos o resguardos de los equipos eléctricos serán construidos e instalados de tal manera que eviten el peligro de conmoción eléctrica o de corto circuito y se dispondrá de acceso seguro a los conductores o equipos a fin de resguardarlos.-

Art. 55.- Cuando se emplean equipos eléctricos portátiles que tengan elementos metálicos al descubierto se tomarán las siguientes medidas:

Los armazones metálicos serán puestos a tierra.

La tensión entre el conductor y tierra, en sistema de corriente alterna o continua no excederá de 200 voltios

Art. 56.- Cuando se efectúe trabajos en las subestaciones de distribución de alta tensión, todo el tablero deberá estar sin corriente, y si está dispuesto en secciones separadas que pueden dividirse y aislarse eléctricamente, solamente la sección pertinente necesitará estar sin corriente.-

Art. 57.- Las lámparas eléctricas portátiles tendrán cubiertas protectoras y se emplean únicamente:

- Cuando no se pueda disponer de lámparas fijas permanente apropiada.
- Con receptáculos o porta lámparas de material aislante y con resguardo adecuado de suficiente resistencia completamente aislado de cualquier elemento a tensión.-
- Con voltaje máximo de 120 voltios ~~en~~ ^{en} lugares secos y 42 voltios en lugares húmedos.- *PH J*



Art. 63.- En todas las máquinas y equipos, se colocarán en sitios apropiados, los procedimientos para su operación incluyendo los de seguridad, los mismo que deben estar indicados en español.

Art. 64.- Todas las partes móviles de las máquinas, motores, transmisores, acoplamientos, etc. Deberán ser protegidas, a menos que estén construidas o colocadas de tal manera que evite que una persona u objeto entre en contacto con ellas.-

Art. 65.- Todos los Operadores y Ayudantes, Auxiliares de la máquinas deben acatar las normas y medidas indicadas en el Manual de Normas de Seguridad Total.-

Art. 66.- Solamente cuando se proceda a efectuar reparaciones de mantenimiento se quitarán los resguardos o dispositivos de seguridad de alguna máquina y se lo colocará inmediatamente después del trabajo.-

Art. 67.- Todos los empleados están en la obligación de dar aviso en forma oportuna e inmediata a sus superiores sobre los defectos o deficiencias que descubran en una máquina, guarda o dispositivo de seguridad.-

Art. 68.- La compañía deberá velar para que toda maquinaria o equipo en general que se compre, venga con su respectivo dispositivo o guarda de seguridad.-

Art. 69.- En toda maquinaria o equipo se buscará la mayor protección posible al sitio de la operación y se dedicará especial atención a la subestación eléctrica, bomba de agua, u otros equipos equivalentes.-

Art. 70.- Las guardas y dispositivo de protección deben ser diseñadas de acuerdo a las Normas indicadas en el Manual de Seguridad.-

Art. 71.- Los montacargas y equipos de limpieza también debe reunir condiciones de seguridad respectivamente.-

Art. 72.- Se comprenderá como materiales de manipuleo, almacenamiento y transporte lo



Art. 76.- Como norma especial de seguridad cuando se planifique el almacenamiento de materiales temporal o permanente no se obstaculizará por ningún concepto o motivo el acceso a los equipos contra incendio.-

Art. 77.- Los cables, cadenas, ganchos y todos los demás accesorios para la manipulación de materiales en el montacargas y equipos equivalentes, deben ser cuidadosamente examinados por el personal de mantenimiento de acuerdo a un programa de inspección.

Art. 78.- No se permitirá que ninguna persona se sitúe debajo de la cargas suspendidas, cables o cualquier elemento de suspensión.


Art. 79.- Para el almacenamiento de materiales se debe utilizar pallets o estanterías metálicas y no dejar los materiales directamente sobre el piso.

Art. 80.- En relación al punto anterior, los conductores de los vehículos de la compañía también deberán observar que las normas de seguridad para este programa se cumplan a cabalidad, tales como:

Inspeccionar todos los días las condiciones Electromecánicas elementales que todo conductor debe conocer (luces, tuercas de las ruedas, aire de las llantas, aceites, etc.).

- ☐ Tener los equipos de emergencia como juego de herramientas, gata, llave de rueda, extintor, botiquín de primeros auxilios, señalización, etc.
- ☐ Controlar la operación de almacenamiento temporal para no exceder de peso.
- ☐ Equipo de protección personal.
- ☐ Equipo para control de derrames.
- ☐ Cumplir con las disposiciones de la Ley de tránsito.-

Art. 81.- Todos los materiales que se almacenen deben estar bien distribuidos considerando normas de espacios, ventilación, altura, compatibilidad, etc.

Art. 82.- Todos los recursos mecánicos utilizados para cumplir con los fines de Agripac S.A., indicados en el artículo 62 deberán ser sometido a un buen sistema de 



Art. 89.- La compañía Agripac S.A. definirá y mantendrá siempre un código de colores normalizado, para aplicarlo según el caso a todos sus recursos en función de sus objetivos.-

Art. 90.- Como referencia de normalización se regirá por lo indicado en el INEN, riesgo del trabajo y Normas ANSI de los Estados Unidos entre otras.-

Art. 91.- El comité y departamento de Seguridad Total de la compañía velará para que se aplique el código de colores, establecidos para pintar o decorar:

- Ambientes de trabajo en general
- Ductos, tuberías y máquinas
- Edificio y estructuras
- Rotulos, letreros y demarcaciones de seguridad, etc.

Art. 92.- Todos los empleados, contratistas y terceras personas respetarán en todo momento, el sistemas de colores de seguridad en lo referente a rótulos, letreros demarcaciones y señalética en general.

Art. 93.- Como complemento al artículo anterior se dará una esencial importancia al sistema de señalización de seguridad contra incendio y emergencias.

Art. 94.- La compañía consciente de que la mayoría de los accidentes no sale afectado el elemento humano, sino los recursos técnicos y materiales, llamados a esta consecuencia daños a la propiedad. considera de vital importancia que estos deben ser eliminados o reducidos a su mas mínima expresión; los daños a la propiedad (DP) tiene la siguientes clasificación:

- Interrupciones y demoras de procesos o actividades productivas
- Daños en los recursos materiales en general
- Otros daños a la propiedad.-



Art. 102.- Los materiales u objetos que ofrezcan riesgos de combustión espontánea como waipes, trapos con: aceites, grasas, pinturas, etc. deben almacenarse en sitios apropiados y se aislarán de otros cuerpos combustibles.-

Art. 103.- Dentro de la Compañía en general es terminantemente **PROHIBIDO FUMAR.-**

Art. 104.- En todos los ambientes de trabajo debe existir elementos, extintores apropiados y en función del área considerada peligrosa.-

Art. 105.- La Compañía a través del Comité y Departamento de Seguridad Total velará para que el sistema de defensa contra incendio, (cisterna, bomba, gabinetes, extintores, etc.) siempre permanezca aptos para controlar este riesgo.-

Art. 106.- De igual forma para controlar riesgo, de incendio de origen eléctrico y electrónico, la Compañía deberá contar con sistema fijos, manuales y automáticos a base de agentes extintores limpios.

Art. 107.- Así mismo, Todos los edificios de la Compañía deberán tener un sistema automático electrónico de alarma o detectores de incendios.

Art. 108.- Todo empleado que observe indicios de propagación de fuego, tiene la obligación de dar alarma y sofocarlos con los medios de extinción que esté a su alcance.-

Art. 109.- El Departamento de Seguridad Total, permanentemente entrenará a los empleados sobre las normas de utilización de estos equipos de tal manera que siempre estén aptos para casos de incendios.

Art. 110.- Todos los empleados en general deben mantener sus áreas y sitios de trabajo, limpios y ordenado para de esta forma eliminar en gran parte la causas de los incendios.

Art. 111.- Cuando ocurra un incendio, el empleado o Jefe está en la obligación de informar inmediatamente al Comité o Departamento de Seguridad Total, quien deberá



Art. 116.- La Compañía a través del Comité y Departamento de Seguridad Total incluyendo la Brigada Contra Incendios y Emergencias mantendrá un plan efectivo de evacuación y contingencias.

Art. 117.- Todos los planos de Evacuación deberán estar siempre ubicados en la parte adyacente de la puerta de escape a la escalera de evacuación u otro sitios estratégicos.

Art. 118.- Es de vital importancia que las escaleras de evacuación reúnan condiciones de seguridad permanentemente tales como:

Libres de Obstáculos

Que tengan lámparas de emergencia por piso y descanso

Ventilación forzada

Señalética normalizada.-

Art. 119.- En general la institución, a través de su Comité y Departamento de Seguridad Total, siempre deberá aplicar sus medidas de intervención, guiándose por las Normas NFPA, de los Estados Unidos entre otras.-

Art. 120.- La Compañía a través de su organización de Seguridad que tiene, velará para que todo el personal de trabajadores conozcan las normas o procedimientos a que está facultado el personal de Vigilancia contratado.-

Art. 121.- El servicio de vigilancia tendrá que cumplir y hacer cumplir todas las normas y disposiciones que imponga la Compañía y contará para esto con un Manual de Procedimiento de Seguridad.-

Art. 122.- Todo el personal al servicio de la Compañía deberá saber que el servicio de Seguridad Física y Vigilancia tiene como objetivo primordial prevenir los DELITOS en general que pudieran presentarse, tales como robo, daños a los recursos materiales, abuso de confianza, secuestro, fraude, atentados, disturbios civiles, etc.

Art. 123.- También deberán saber que el personal de Vigilancia ubicado en las puertas de entrada o salida controla los ingresos y egresos de personal, y materiales; así como también



CAPITULO V

SOBRE SALUD OCUPACIONAL

Art. 130.- La Compañía considera que la Seguridad Total es relativa y que es una gestión multidisciplinaria y que fortalecer la protección de su recurso humano contra enfermedades comunes y principalmente profesional se requiere de la participación efectiva del servicio de la misma.-

Art. 131.- El Servicio Médico de la compañía bajo el control de la Gerencia de Recursos Humanos debe estar entrenado en la aplicación de la Medicina Preventiva y del Trabajo, para lo cual entre otras tareas hace:

- Inspecciones periódicas a los sitios de trabajo.
- Charlas al personal.
- Análisis y recomendaciones de prevención de riesgos.
- Revisión de la ficha médica anual.
- Informar al Comité de Seguridad Total sobre condiciones insalubres de trabajo.-

Art. 132.- El Departamento de Seguridad Total y el Servicio Médico coordinarán efectivamente para la prevención de riesgos de enfermedades ocupacionales.-

Art. 133.- Todos los empleados al servicio de esta compañía, están obligados a observar y cumplir las medidas de higiene personal que prescriba la Ley, los reglamentos, manuales de procedimientos internos, instrucciones o procedimientos personales y colectivos de sus colaboradores.

Art. 134.- Entre las principales medidas que todo el personal deberá observar serán las siguientes:

- Presentarse a sus labores en condiciones de aseo y limpieza.
- Mantener limpio y ordenado su puesto de trabajo.
- Utilizar en forma correcta los servicios sanitarios.



Art. 143.- Los oficinas, bodegas y plantas en general, deben estar provistos de iluminación artificial con intensidad uniforme y distribuida de tal manera que cada máquina, equipo, banco de trabajo o lugar donde se realice alguna labor, funcione sin que se proyecten sombras o produzcan deslumbramientos.-

Art. 144.- La iluminación artificial debe estar de acuerdo con el nivel mínimo de iluminación en luces conocidos internacionalmente e indicado en el Reglamento de Seguridad e Higiene del Trabajo del Instituto Ecuatoriano de Seguridad Social.-

Art. 145.- El ruido en los sitios de trabajo u otros lugares de preferencia se lo debe eliminar en la fuente, debiéndose completar esta medida de seguridad con el uso de los equipos protectores contra el ruido, considerando los niveles sonoros máximos admisibles.

Art. 146 - De igual forma se considerará de importancia a los riesgos de vibraciones y radiaciones para su control efectivo.

Art. 147 - El Comité y Departamento de Seguridad Total velarán para que en todas las oficinas, bodegas, terrazas, sótanos, etc los trabajos se desarrollen dentro del mismo HOMBRE MAQUINA normal.

Art. 148.- El personal con mando en general de la Compañía, controlará que en el departamento o área bajo su supervisión no se detecte:

- Sobreesfuerzo de trabajo
- Sobrecargas de trabajo.
- Fatiga.
- Estrés

Art. 149.- De igual forma el personal con mando en coordinación y bajo el asesoramiento del departamento de Seguridad Total en todo instante velará para que siempre el recurso material que se utiliza en su área sea apto para sus colaboradores, es decir que la tendencia sea de adaptar el ambiente de trabajo con todos sus recursos al hombre para prevenir enfermedades comunes y profesionales fundamentalmente. *H. J.*



- Cambios en el Producto.
- Control de la Fuente.
- Técnica de Control Ambiental

Art. 157.- De igual forma. la Compañía cumplirá con las disposiciones emitidas por la Municipalidad de Guayaquil, y demás Leyes pertinentes para no contaminar el ambiente.

Art. 158.- Todos los empleados en general acatarán lo indicado en el Manual de Seguridad Total, en lo que a Seguridad Ambiental se refiere.

CAPITULO VII

DISCIPLINA, OBLIGACIÓN Y SANCIONES

Art. 159.- Todo empleados al servicio de la Compañía Agripac S. A., deberán cumplir todas las normas y medidas de seguridad que se dictaren, y el incumplimiento de las mismas sean generales daño de la instalaciones, maquinarias o equipos, etc. Por lo expuesto para evitar cualquier sanción siendo la máxima la terminación del contrato por incumplimiento, los trabajadores están obligados a cumplir en su totalidad este reglamento según consta en el artículo número 416 del Código del Trabajo.

Art. 160.- El área de Recursos Humanos y Servicios es la responsable de calificar las infracciones y determinar las sanciones, así la condición de negligencia de cualquier acto u omisión que signifique trasgresión al presente reglamento.

Art. 161.- Es obligación de todo trabajador solucionar si está a su alcance o informará enseguida al jefe inmediato sobre cualquier defecto a descubrirse en cualquier ambiente de trabajo de la empresa.

Art. 162.- Todos los trabajadores deberán cumplir normas y medidas de prevención de riesgos determinados por el Comité de Seguridad Total debiendo en todo momento cooperar en el cumplimiento de este reglamento y las que se dicten en el futuro.

CONSORCIO JURÍDICO VELARDE & ASOCIADOS

Oficina General Córdova No. 623 y Padre Solano
Telf. 042-560400, Ext. 228.- Cel. 099422289
Guayaquil - Ecuador

DIRECTORA REGIONAL DE TRABAJO DEL LITORAL.- ABOGADA MARTHA MANSSUR CASTAÑEDA.-

Econ. IVAN EDUARDO NOBOA IZURIETA, por los derechos que represento de la compañía AGRIPAC S. A., en calidad de Primer Gerente y Representante Legal, lo que legítimo con el nombramiento adjunto a la presente, ante usted comparezco solicito y digo:-

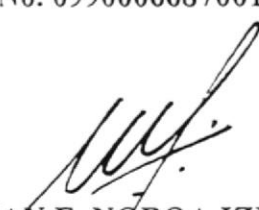
PRIMERO: AUTORIZACIÓN Y NOTIFICACIÓN.- Autorizo al profesional del derecho abogado CARLOS D. VELARDE VILLÓN, para que a mi nombre y representación presente cuantos escritos sean necesarios en el presente tramite. Para futuras notificaciones se me las haga en la casilla judicial 262 en los bajos del Palacio de Justicia de Guayaquil.-


SEGUNDO: PETITORIO.- Señora Directora de Trabajo, sírvase encontrar adjunto a la presente TRES REGLAMENTO DE SEGURIDAD, HIGIENE Y SALUD DE LOS TRABAJADORES Y MEJORAMIENTO DEL MEDIO AMBIENTE DE TRABAJO DE LA COMPAÑÍA AGRIPAC S. A., para su revisión, aprobación, legalización y registro.-

Petición que realizo en cumplimiento a lo estipulado en el Artículo 441 del Código de Trabajo vigente, en concordancia con el Decreto Ejecutivo No. 2393 en el Registro Oficial No. 565 de fecha 17 de Noviembre de 1986.-

Dígnese proveer lo peticionado por ser de estricto derecho.-

Por la Compañía AGRIPAC S. A.
R. U. C. No. 0990006687001.-


Econ. IVAN E. NOBOA IZURIETA
PRIMER GERENTE


Ab. CARLOS VELARDE VILLÓN
MATRICULA No. 10.672 C. A. G.-

DIRECCION REGIONAL DEL TRABAJO
REGISTRO DE DOCUMENTOS
Hora: 14:15
Fecha: JUNIO 29-05
Firma: Jani



Art. 168.- La inobservancia de las medidas de prevención de riesgos, establecidas en el presente reglamento, constituye causa legal para la terminación del contrato con el trabajador, de acuerdo a lo dispuesto en el artículo ~~174~~ del Código de Trabajo.-

172

Art. 169.- El incumplimiento de las recomendaciones medicas será motivo de sanción.-

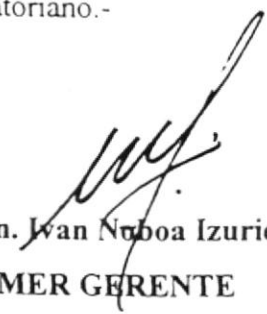
Art. 170.- El incumplimiento de las normas estipuladas en los reglamentos de seguridad vigente, dará lugar a las siguientes sanciones:

1. Amonestación por escrito.
2. Multa pecuniaria de hasta el 10% de la remuneración día.
3. Terminación del Contrato de trabajo previo Visto Bueno. Esta sanción en ningún momento se considerará en orden de prioridad sino en atención a la gravedad y a criterio de la compañía AGRIPAC S. A.

CAPITULO IX

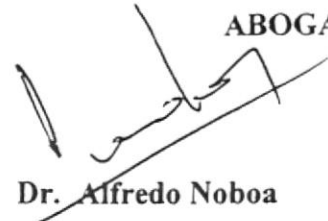
DISPOSICIÓN FINAL

Art. 171.- Este Reglamento de Seguridad Salud y Ambiente de la Compañía AGRIPAC S. A., se entenderá conocido y aceptados por todos los trabajadores de la empresa y entrará en vigencia desde la fecha de su aprobación por parte de la Dirección ^{Regional} de Trabajo y será exhibido en un lugar visible, dentro de la empresa y sucursales dentro del territorio ecuatoriano.-


Econ. Ivan Noboa Izurieta
PRIMER GERENTE


Carlos Velarde Villón.

ABOGADO MATRICULA 10672


Dr. Alfredo Noboa
Asesor de Salud Ocupacional



**SUBSECRETARIA DE TRABAJO DEL LITORAL Y GALAPAGOS
DIRECCION REGIONAL DEL TRABAJO**

Guayaquil

Ecuador

DIRECCIÓN REGIONAL DEL TRABAJO

Guayaquil, 22 julio del 2005, las 14h50

De conformidad con el Art. 441 del Código del Trabajo, se aprueba, el Reglamento de Seguridad de Higiene Industrial de la Compañía **AGRIPAC S.A.**, el mismo que regulará las relaciones laborales con sus trabajadores, con las siguientes modificaciones: En el Art. 4, eliminar "se"; Art. 57, inciso cuarto sustituir "el" por "en"; Art. 113, inciso primero sustituir "otros" por "otras"; Art. 164, inciso primero, después de "que" agregar "están"; Art. 168, suprimir "174" por "172"; Art. 171, después de "Dirección" agregar "Regional";.- Actúe la Abg. Zoila Delvicier Mejía, Secretaria Regional del Despacho, quién pondrá las certificaciones respectivas, archivará el original y entregará las copias de conformidad con la Ley. Exhibase un ejemplar legalizado del presente reglamento en un lugar visible de la Compañía, para que sea conocido por todos los trabajadores.- **CÚMPLASE Y EXHÍBASE.-**

Ab. Martha Manzur Castañeda
**DIRECTORA REGIONAL DE TRABAJO Y
MEDIACION LABORAL DEL LITORAL Y
GALAPAGOS**



LO CERTIFICO:

Ab. Zoila Delvicier Mejía
SECRETARIA REGIONAL
Dirección Regional del Trabajo

CERTIFICO: Que el Reglamento de Seguridad e Higiene Industrial de la Compañía **AGRIPAC S.A.**, queda registrado en el libro respectivo, archivándose el original y entregándose copias de conformidad con la ley.

Guayaquil, 22 de julio del 2005

Ab. Zoila Delvicier Mejía

ACCESO FISICO

El área de sistemas por ser un área de acceso restringido está ubicada en el último piso del edificio del área contable financiera de la organización, además de las seguridades que se mantienen en la empresa para permitir el ingreso de las personas, el área de sistemas cuenta con su propio procedimientos para evitar que personas ajenas a la organización y personal interno no autorizado tengan acceso a este departamento.

La única puerta de acceso al piso permanece cerrada con una cerradura eléctrica, se cuenta con un intercomunicador a través de cual las personas no autorizadas se comunican con la asistente de la gerencia de sistemas, quien después de realizar la consulta respectiva determina si se permite el ingreso o no de la persona que se anuncia.

El piso cuenta con un sistema de alarma que controla la puerta de ingreso y además tiene sensores de movimientos para detectar el acceso de intrusos cuando no hay nadie en el piso, al mismo sistema están conectados los sensores de humo que alertarán mediante la sirena en caso de un principio de incendio, igualmente se mantienen varios extintores de incendio ubicados estratégicamente en el piso. Todo el sistema de seguridad es monitoreado remotamente por una empresa de seguridad que lleva una bitácora de control de acceso y salida por cada persona de sistema que activa y desactiva la alarma, para ello se asignó una clave a cada miembro del equipo de sistemas.

El acceso físico al centro de computo está restringido solo para personas autorizadas las que previamente son identificadas por la asistente de la gerencia de sistemas quien controla el interruptor que acciona la chapa eléctrica que permite ingresar al piso.

La sala de máquinas donde están los servidores se encuentra cerrada con llave y el acceso a ella es totalmente restringido permitiéndose el ingreso solo a personal autorizado, quienes después de justificar el motivo de ingreso deben registrarse en una bitácora que se encuentra junto a la puerta de acceso, en dicha bitácora se registra el nombre de la persona, la fecha, hora, motivo del ingreso y hora de salida.

PROCEDIMIENTO PARA CONFIGURAR REPLICACION DE LAS BASES DE DATOS ONLINE 7.2X

Para efectos de definir la replicación es necesario establecer cual es el servidor primario y cual el servidor secundario.

Los pasos que se describen a continuación deben ser ejecutados en el orden descrito en este manual, y en el servidor que corresponda:

- 1.- Servidor primario Respaldar la base en nivel 0
\$ ontape -s -L 0
- 2.- Servidor primario Definir este motor de base de datos como primario
\$ onmode -d primary nombre_servidor_secundario
- 3.- Servidor secundario Recuperar el respaldo de nivel 0 con el comando
\$ ontape -p
Este comando pregunta se desea respaldar los
Logical logs, hay que responder NO
- 4.- Servidor secundario Definir este motor como secundario
\$onmode -d secondary nombre_servidor_primario

Para poder comprobar que esta funcionando la replicación se debe ejecutar el comando
\$ onstat -g dri

El resultado de este comando en el servidor primario debe ser el siguiente:

```
INFORMIX- OnLine Version 78.23.UCL        — Prim (UP)    00:29:33    — 982880 Kbytes
```

Data Replication:

Type	State	Paired server	Last DR	CKPT (id/pg)
Primary	on	agripac2		8745/8745

```
DRINTERVAL    30  
DRTIMEOUT    30  
DRAUTO        0  
DRL0STF0UND   /f/informix7/etc/dr.lostfound
```

El resultado de este comando en el servidor secundario debe ser el siguiente:

```
INFORMIX- OnLine Version 78.23.UCL        — Secondary (UP)    00:29:33    — 982880 Kbytes
```

Data Replication:

Type	State	Paired server	Last DR	CKPT (id/pg)
Secondary	on	agripac		8745/8745

```
DRINTERVAL    30  
DRTIMEOUT    30  
DRAUTO        0
```


Como podemos apreciar el estado de ambos servidores debe ser ON, en caso de que el estado este en OFF, y no logren los servidores sincronizar la replicación, se debe repetir este proceso.

También es importante que revisemos el archivo ONLINE.LOG para poder entender el paso a paso lo que el motor de la base de datos realiza cuando se habilita la replicación.

Para esto ilustrare en cada paso lo que se adiciona en el archivo online.log cuando se ejecuta cada comando:

- 1.- Servidor primario
Respaldar la base en nivel 0
Level 0 archive on rootdbs datadbs indexdbs Started

Level 0 archive on rootdbs datadbs indexdbs Completed
- 2.- Servidor primario
Definir este motor de base de datos como primario
DR: New type primary, secondary server name = agripac2
DR: Trying to connect to secondary server
DR: Cannot connect to secondary server
- 3.- Servidor secundario
Recuperar el respaldo de nivel 0 con el comando
INFORMIX – OnLine initialized - - Shared memory
Initialized
Recovery mode
Physical restore of rootdbs datadbs indexdbs Started
Physical restore of rootdbs datadbs indexdbs Completed
- 4.- Servidor secundario
Definir este motor como secundario
DR: New type = secondary , primary server name = Agripac
DR: Trying connect to primary server
DR: Secondary server connected
DR: failure recovery from disk in process
Logical Recovery allocating n worker threads (“OFF_ RECVRY_THREADS”)
Logical recovery Started
Start Logical Recovery – Start Log n , End Log?
Starting Log Position - n 0xnxxxxx
DR: Secondary server operational
- 5.- Servidor primario
DR: Primary server operational

PROCEDIMIENTO PARA HABILITAR EL SERVIDOR SECUNDARIO

En caso de tener alguna contingencia en el servidor principal, también definido como servidor primario, y que el servidor secundario este operativo y replicando hasta el momento mismo de la caída del sistema, es necesario que se sigan estos pasos para poner el servidor secundario como primario.

- 1.- Cambiar el estado del motor de la base de datos a STANDARD, ejecutando como usuario informix el siguiente comando:
\$ onmode -d standard
- 2.- Bajar el motor de la base de datos con el comando:
\$ onmode -ky
- 3.- Cambiar el nombre del servidor como usuario root, con el siguiente comando:
uname -S agripac
- 4.- Editar los archivos /etc/rc.d/8/userdef y /etc/shutdown.d/informixdown cambiando el nombre de la variable INFORMIXSERVER=agripac
vi /etc/rc.d/8/userdef
vi /etc/shutdown.d/informixdown
- 5.- Cambiar la dirección IP del servidor a 10.2.1.12, ejecutando el comando:
netconfig
Este comando pedirá regenerar el KERNEL del unix
- 6.- Reiniciar el servidor utilizando el comando:
shutdown -y -g0 -i6

PROCEDIMIENTO PARA CARGA DEL SISTEMA OPERATIVO SCO UNIX OPENSERVER ENTERPRISE

Objetivo

La finalidad de este instructivo es conocer todos los pasos que deben ser ejecutados a fin de cargar el sistema operativo, definir todos los periféricos y dispositivos, cargar datos y aplicaciones, y todos los directorios necesarios que permitan a los usuarios de la empresa ejecutar sus procesos diarios.

Procedimientos

Antes de conocer los pasos es necesario tener a disposición información importante que nos permitirá cumplir con el objetivo.

En el casillero de seguridad del banco Bolivariano, se encuentran diskettes que contienen drivers que deben ser cargados al momento de la instalación, diskettes con información de archivos que nos indican las impresoras que estaban instaladas, los usuarios, además, hay cintas con información de directorios y filesystems que deben ser restaurados luego de finalizada la instalación.

Los filesystems deben ser restaurados, si en el proceso de instalación estos no pueden ser preservados, caso contrario, no es necesario crearlos.

1. Encender el equipo cargando desde el CD de instalación del sistema operativo.
2. cuando muestre el Boot: ingresar la palabra "link"
3. El sistema pedirá el nombre del driver, poner "amird" e ingresar el diskette con el driver
4. El sistema hará un reconocimiento de todo lo que detecte
5. Pedirá el ingreso del número de licencia
6. Para la red detectará la tarjeta y pedirá una dirección IP.
7. En el caso de ser una reinstalación, preguntará si desea preservar los otros filesystems que detecte en el sistema
8. Luego de esto procederá a cargar todo el sistema operativo
9. Al finalizar, reiniciará el equipo, y se deberá retirar los diskettes y CD'S que estén en el equipo antes de reiniciar.
10. Una vez que reinicio sin problemas, hay que verificar los filesystems que fueron preservados
11. Los filesystems que faltan deben ser adicionados, y su información restaurada desde cinta
12. Instalar software adicional como SCO SMP para manejo de otro procesador
13. Instalar los suplementos de actualización que tenga la versión del sistema operativo, para esto es necesario ingresar a la página web www.sco.com
14. Instalar los usuarios desde el diskette utilizando el comando ap
15. Configurar las impresoras tomando la información del diskette
16. Instalar las licencias de usuarios adicionales
17. Cambiar los parámetros de afinamiento del sistema en el archivo "stune", el mismo que está respaldado en los diskettes
18. Cargar el driver de la controladora raid "iir" con el comando `installpkg`

19. Agregar las unidades lógicas configuradas en el raid con el comando `mkdev hd`
20. Crear las 43 particiones o filesystems que corresponden a los chunks de la base de datos
21. Configurar la unidad de tape backup con el comando `mkdev tape`
22. Reiniciar, el servidor estará listo para instalar la base de datos

PROCEDIMIENTO PARA INSTALAR EL MOTOR DE LA BASE DE DATOS

Objetivo

Con este instructivo pretendemos documentar los pasos necesarios para instalar el motor de la base de datos, inicializar la base y restaurar la información.

Procedimientos

1. En el sistema operativo crear el usuario "informix" y que pertenezca al grupo "informix".
2. Bajar de cinta el directorio /f/informix7, que contiene el software
3. Restaurar el archivo onconfig al directorio /f/informix7/etc/onconfig que contiene los parámetros de instalación de la base de datos
4. Inicializar la base de datos con el administrador del motor "onconfig"
5. En esta instancia se crea el "rootdbs" en el dispositivo "/dev/rchkdsa0" con un tamaño de 1998976MB y con un área de offset de 1024K con lo que completamos los 2GB que es el tamaño máximo de cada chunk
6. Proceder a agregar cada uno de los 43 chunks
7. Los "dbspaces" que deben haber en el sistema son:
 - Rootdbs con 2 chunks
 - Logdbs con 1 chunk
 - Logdbs1 con 1 chunk
 - Tempdbs0 con 1 chunk
 - Tempdbs1 con 1 chunk
 - Datadbs con 25 chunks
 - Indexdbs con 12 chunks
8. Cada chunk debe ser igual en tamaño al rootdbs, 1998976MB y 1024K de offset
9. Agregar logs hasta completar 66 en sus respectivos dbspaces (logdbs, logdbs1)
10. Agregar los servicios de informix al archivo /etc/services
11. En el directorio /dev cada chunk debe pertenecer al usuarios "informix" y al grupo "informix"
12. Cada chunk debe tener el permiso 660
13. Una vez creados los chunks, restaurar desde cinta el nivel 0 de la base de datos con el comando ontape -r

Tiempo estimado

El proceso de creación y restauración de la base de datos es de 7 horas aproximadamente

PROCEDIMIENTO PARA CARGA DEL SISTEMA OPERATIVO WINDOWS 2000 SERVER

Objetivo:

Con este instructivo pretendemos documentar los pasos necesarios para instalar el sistema operativo Windows Server 2000 con los productos necesarios que permita el adecuado funcionamiento de la red manteniendo las seguridades requeridas.

Procedimientos

Antes de proceder a la instalación de los productos se debe tener el diseño de la red para determinar que productos deben ser instalados y los criterios para la parametrización de cada una de los servicios.

Igualmente se debe tener claramente identificado los servicios que no se desean instalar especialmente aquellos de uso restringidos para evitar que puedan ser utilizados de manera indebida ocasionando perjuicio a la red, ejemplo telnet, ftp, IIS (WEB).

Instalación del Sistema

Para la instalación de **Windows 2000** se debe seguir de los siguientes pasos:

Ejecutar el Programa Setup.

Antes de que aparezca la ventana de instalación (Wizard) el asistente advertirá si se desea convertir el sistema de archivos **FAT** ó **FAT32** a **NTFS**, se recomienda instalar el sistema de archivos **NTFS** el cual permite utilizar eficientemente las funciones de administración de archivos, además de contar con mayor seguridad en cuanto a permisos.

Durante el proceso de instalación de **Windows 2000**, el programa pregunta por el dispositivo de disco que utilizará para la instalación. Se puede elegir formatear una partición y hacerla **NTFS**. En caso de no realizarla hay varios métodos para convertir una partición a **NTFS**.

Ejecutar el Setup Wizard.

El proceso inicia simplemente ejecutando el archivo de **Setup**. El cual aparece una ventana de instalación (**Wizard**), seguir con las indicaciones hasta la opción (optional components), desde este momento se debe ir seleccionando de acuerdo a su diseño de requerimientos en su sistema los servicios a instalar.

Instalar los Servicios de Windows 2000.

Windows 2000 ofrece opciones predeterminadas de instalación rápida pero se recomienda nunca elegir una opción predeterminada, el hacerlo es aceptar que instale todo lo que la distribución del producto (Microsoft) cree que es indispensable, pero como ya se había mencionado es recomendable instalar sólo los servicios necesarios.

Cuando se esta creando un servidor seguro, se deben elegir sólo los componentes que sean necesarios, por ejemplo:

¿Para que instalar los componentes **HyperTerminal** o **Marcador telefónico** si el servidor no va a permitir el acceso mediante **MODEM**?

Cualquier programa que no se necesite puede ser un blanco potencial para un "intruso", podría esconder algún caballo de Troya por mencionar un ejemplo.

Completar el Programa de Instalación.

La versión de **Windows 2000** es capaz de reconocer y dar soporte a una multitud de dispositivos, asignando de forma automática los recursos e instalando los controladores, esto es por el reconocimiento **Plug and Play**.

A partir de la versión **Server** y **superiores**, el administrador de la red tiene la opción de realizar la instalación de **Windows 2000** de forma remota sobre las máquinas **clientes**.

Iniciando por Primera Vez

El sistema se encuentra ya instalado, ¿la computadora está lista? La respuesta es ¡NO! aún no está lista para salir a la red, es necesario tenerla desconectada ya que la máquina esta demasiado expuesta aún.

Al acabar de instalar el sistema operativo, todavía no se ha cerrado ningún servicio que se instala por **default** (En el caso de haber hecho una instalación por **default**). No se han aplicado los parches para corregir errores del sistema. El sistema aún no tiene instaladas herramientas de seguridad que ayudarán a fortalecer nuestro sistema.

Es recomendable hacer pruebas antes de conectar la máquina a la red, ya que de no hacerlo no se puede verificar la funcionabilidad, confiabilidad y operatividad del sistema.

Uno de los conceptos de seguridad dice "**no mantener servicios abiertos que no sean indispensables.**"

Windows 2000 viene con varios puertos abiertos por **default**, estos tienen que ser cerrados para evitar que estos sean utilizados, ya que cualquier servicio puede tener algún hueco de seguridad (**bug**) escondido, otro punto fundamental en la seguridad es que cuantos más servicios se estén prestando, más riesgo se corre que alguna vulnerabilidad sea encontrada y explotada.

Los protocolos de **Windows 2000** que presentan un problema de riesgo adicional de seguridad son los servicios **FTP**, **Telnet** ya que estos servicios requieren contraseña, esta es transmitida en texto claro por lo que abre la posibilidad de que algún atacante este escuchando en la red y así pueda capturar dichas contraseñas lo cual es un grave riesgo a nuestro sistema, por lo que estos servicios deben permanecer cerrados.

Los pasos a seguir son:

- 1.- **Star/Settings/Control panel**
- 2.- **Add/Remove Programs/Add/Remove Windows Components**
- 3.- **Windows Components Wizard**

4.- Si está activada una casilla de verificación de un componente, el componente está instalado. Para eliminar un componente desactive la casilla y haga clic en siguiente

5.- Si es necesario eliminar un subcomponente, seleccione y haga clic en él, puede anular desactivando el subcomponente.

6.- Dependiendo del componente, aparecerá otro cuadro de dialogo, mostrando el proceso de eliminación del componente. Haga clic en **Finalizar** cuando el programa lo solicite.

Para verificar los servicios abiertos se usa el comando **net start** para verificar los servicios que están activos y comprobar que efectivamente sólo tenemos los que necesitamos.

Los servicios que no son necesarios en un servidor seguro son:

- **FTP**
- **Web** (solo en caso de ser servidor web).
- **Telnet**

Estos servicios son los más atacados ya que presentan grandes huecos de seguridad.

Políticas de Cuenta

Para establecer las políticas de cuenta se presenta el cuadro de seguridad de acuerdo a las necesidades de la organización.

1.- Inicio/Programas/Herramientas Administrativas/Local Security Policy\

2.- Expandir **Account Policies**, click en **Password Policy**(política de contraseña)

El cuadro siguiente tiene las políticas de seguridad en base al nivel básico, seguro, o seguridad máxima.

Política	Básico	Segura Media	Seguridad Avanzada
Política de cuenta			
Política de Contraseña			
Forzar historial de contraseñas (Password History Size)	No definido	4 contraseñas recordadas	24 contraseñas recordadas
Máxima edad de las contraseñas(MaximumPasswordAge)	No definido	42 días	42 días
Minima edad de contraseñas MinimumPasswordAge)	No definida	2 días	2 días
Minima longitud de contraseñas Minimum PasswordLength)	No definido	8 caracteres	8 caracteres
Las contraseñas deben cumplir los requisitos de complejidad PasswordComplexity)	No definido	Habilitado	Habilitado
Guardar contraseñas utilizando cifrado irreversible para todos los usuarios (ClearTextPassword)	No definido	Deshabilitado	Deshabilitado
Políticas de bloqueo de cuentas			
Duración del bloqueo de cuentas (LockoutDuration)	No definido	30 minutos	0
Límite del bloqueo de cuentas (LockoutBadCount)	No definido	5 intentos de inicio de sesión no válidos	5 intentos de inicio de sesión no válidos
Reinicializar el contador de bloqueo después de (ResetLockoutCount)	No definido	30 minutos	30 minutos

Windows 2000 puede auditar un gran número de sucesos en el sistema que se dividen en tres registros.

- Aplicación

- Sistema
- Seguridad

Para controlar las propiedades del archivo de registro de auditoria se puede ver en:

- 1.- Inicio/Programas/Herramientas Administrativas/Visor de Sucesos (Event Viewer).
- 2.- Seleccionar cualquiera de los registros.
- 3.- Click/botón derecho del mouse propiedades del registro.
- 4.- Aparecerá el cuadro de propiedades donde vienen la información General del registro:

- El nombre del registro
- La base de datos donde se guarda la información de los sucesos auditados
- El tamaño actual de la bitácora, la fecha de creación, modificación y Acceso.
- El tamaño máximo del archivo log(bitácora) por default 512 KB, pero puede ser más grande o más pequeña (tamaño mínimo 64K) según sean las necesidades.
- Configuración cuando alcance el tamaño máximo del registro
- Sobrescribir sucesos cuando sea necesario.
- Sobrescribir sucesos más antiguos de (7 días predeterminados).
- No sobre escribir sucesos (limpiar el registro (bitácora) manualmente).

Hasta este punto tu sistema ya esta instalado, aplicando los parches, asegurado y listo para conectarse a la red (Internet).

INTERRUPCION DE ENERGÍA ELÉCTRICA

Los servidores de la organización así como los enlaces que conectan a las redes y usuarios remotos necesitan y funcionan las veinticuatro horas del día durante todo el año, por lo tanto es imprescindible contar con un sistema alternativo de abastecimiento de energía eléctrica, los cortes de corto tiempo son mitigados con equipos de UPS de 4 KVA que permite seguir funcionando los servidores durante 20 minutos en caso de interrupción del fluido eléctrico mayor a 10 minutos la organización cuenta con un generador de energía que cubre la demanda de toda la empresa, el mismo que está listo para entrar en funcionamiento, para lo cual se debe seguir el siguiente procedimiento.

1. Se debe mantener combustible para el funcionamiento del generador durante ocho horas como mínimo.
2. Las baterías deben ser revisadas constantemente para asegurarse que tengan la carga suficiente que permita encender el generador en cualquier momento y a cualquier hora.
3. El responsable de cumplir con los dos puntos anteriores es el electricista que brinda este tipo de servicio en la compañía.
4. El encendido del generador, está a cargo del electricista a falta de éste el señor Manolo Viera, o el jefe de guardias de la empresa.
5. Antes de encender el generador se debe constatar que el breaker master que está al lado de generador esté en OFF.
6. Se enciende el generador, se constata el voltaje que esté entre los parámetros establecidos 120 voltios +- 2%.
7. Se mantiene encendido durante un minuto para que se estabilice el funcionamiento.
8. Se procede a cambiar la posición del breaker master a ON.
9. Se realiza el cambio de breaker en cada uno de los edificios, para habilitar el suministro de energía desde el generador en reemplazo de la energía de la empresa eléctrica, este sistema tiene un seguro que no permite mantener ambos breaker en posición ON, se necesita deslizar manualmente el seguro desde un lado a otro para poder hacer el cambio de posición de los breaker. Esta operación se la debe realizar en cada edificio, estando bajo la responsabilidad de las personas mencionadas en el numeral 4.

10. Una vez restituido el servicio de energía por parte de la empresa eléctrica, se procede a realizar el cambio de posición de los breaker con el mismo procedimiento detallado en el inciso 9, posteriormente se baja el breaker master y luego se apaga el generador.

PROCEDIMIENTOS DE RESPALDOS

Objetivo

Este es una de las tareas mas importantes, ya que los datos respaldados, sirven para recuperar información en casos de siniestros o de cualquier contingencia que se presente.

Para esto identificaremos 3 tipos de respaldos:

- Respaldo del sistema operativo
- Respaldo de directorios y filesystems
- Respaldo de la base de datos

Respaldo del sistema operativo

El respaldo del sistema operativo copia en formato "CPIO" el filesystem /dev/root, y nos sirve en casos de perder algún archivo del sistema para recuperarlo desde esta cinta.

Procedimiento

1. Ingresar al sistema como usuario root
2. poner la cinta en la unidad de tape backup
3. ejecutar el comando "scoadmin" que realiza tareas de administración del sistema.
4. Escoger la opción de backup, mostrando todos los filesystems del sistema, permitiéndome seleccionar el /dev/root
5. Ingresar información del tape backup sobre factor de bloqueo 102450K
6. una vez terminado el respaldo, la cinta debe ser etiquetada, identificando el tipo de información que contiene.
7. Este respaldo debe ser actualizado por lo menos una vez al mes, o cada que el sistema operativo sea actualizado
8. Llenar el bitácora registrando información sobre este respaldo
9. Llevar la cinta al casillero de seguridad el banco Bolivariano

Respaldo de directorios y filesystems

El respaldo de directorios y filesystems, nos permite guardar información correspondiente a perfiles de usuarios, software de la base de datos, aplicación, datos de prueba, etc.

Procedimiento

1. Ingresar al sistema como usuario root
2. Poner la cinta en la unidad de tape backup
3. ejecutar el comando: tar -cv8 /c /d /e /f /u /prg
4. Una vez terminado el respaldo, la cinta debe ser etiquetada identificando el tipo de información que contiene
5. Este respaldo debe ser actualizado por lo menos 1 vez a la semana.
6. Llenar el bitácora registrando información sobre el respaldo

7. Llevar la cinta al casillero de seguridad del banco Bolivariano

Respaldo de la base de datos

El respaldo de la base de datos nos permite guardar información correspondiente a transacciones que se generan en el sistema Elite.

Procedimiento

1. Ingresar al sistema como usuario "informix"
2. Poner la cinta en la unidad de tape backup
3. Ejecutar el comando "ontape -s -L 0", con esto sacamos un respaldo a nivel 0 de la base de datos, esto quiere decir que es un respaldo total de la base.
4. Una vez terminado el respaldo, la cinta debe ser etiquetada identificando el tipo de información que contienen
5. Este respaldo debe ser ejecutado diariamente
6. Llenar el bitácora registrando información sobre el respaldo
7. Llevar la cinta al casillero de seguridad del banco Bolivariano

PROCEDIMIENTO PARA LA ASIGNACIÓN Y USO DE CLAVES PARA TENER ACCESO A LOS SISTEMAS DE INFORMACIÓN

ACCESO LOGICO:

La clave es la llave para tener acceso al activo más valioso de la empresa que es la información. El uso de las claves es estrictamente personal e intransferible y no debe ser divulgada ni prestada a ninguna otra persona por ningún motivo, ya que la responsabilidad por el uso indebido de una clave es exclusivamente del usuario dueño de la clave.

Por seguridad hemos establecido como política que las claves caducarán cada mes, el sistema obligará cambiar la clave a todos los usuarios. El tamaño del password o clave estará conformado como mínimo por seis caracteres entre letras y números.

Si algún usuario sospecha que su clave es conocida por otra persona debe solicitar vía correo al administrador de la red Sr. Carlos Suarez, (con copia a esta gerencia) el inmediato cambio de clave, para ello se procederá a caducar la clave y el sistema exigirá al propio usuario ingresar la nueva clave cuando inicie una nueva sesión, de esta manera ni el administrador conocerá la clave de ningún usuario.

Está terminantemente prohibido instalar en las estaciones de trabajo (PC) software o programas no autorizado de ningún tipo.

Se mantendrá un constante monitoreo sobre el tráfico y sitios visitados por los usuarios que tienen correo externo y acceso a Internet.

El uso de la información es exclusivamente para realizar actividades y tareas que estén alineados con los objetivos de la empresa. Se realizará una revisión para que cada usuario tenga acceso a la información estrictamente necesaria para realizar su trabajo.

AGRIPAC s.a.

Sistemas y Comunicaciones

Solicitud de servicios: Instrucciones de uso

El formulario S6, es el instrumento que utilizarán los jefes de área de la corporación para requerir del área de Sistemas, equipos de computación y comunicación, así como, autorización para acceder a programas de comunicación y datos, para sí mismos o para sus subalternos. Para lo cual, deberán escribir la siguiente información:

Tipo de servicio.- El tipo de servicio, debe ser marcado como "Cuenta Nueva" o "Dar de Baja" si se trata de un compañero que acaba de ingresar o salir, respectivamente; en los demás casos, debe marcarse "Mantenimiento". A continuación, el jefe de área deberá indicar:

Nombre Usuario .- Nombre del usuario;
Departamento .- Nombre del departamento;
Sucursal .- Nombre de la sucursal;
Fecha de Solicitud.- Fecha de elaboración.

La "Fecha de Recibido" como la "Fecha de Trámite" deben ser dejados en blanco, ya que son de uso exclusivo del área de Sistemas.

En la caja "Use solo para mantenimiento" se deberá escribir la siguiente información:

Nombre Usuario .- Nombre del usuario en RED;
Departamento .- Nombre del departamento;
Nombre de Cuenta.- Nombre de la cuenta en ELITE;
Menú de Datos .- Nombre del menú de ELITE;
Otro servicio .- Nombre de servicios adicionales.

En la caja "Servicios Solicitados" se escribirá una "X" debajo del título "Marque X" en cada una de las celdas que se correspondan a los servicios solicitados.

En ningún caso, se ingresará información en la sección denominada "Reservado para uso de Sistemas"; pero se podrá anotar información adicional, a la derecha del título "Observación".

En toda solicitud, deberá constar el nombre y la firma del jefe de área que solicita el servicio.

Una vez aceptado el requerimiento de servicio por el área de Sistemas y Comunicaciones, se procederá a su asignación a los Administradores del Sistema, luego de los cual, se notificará vía e-mail al usuario solicitante, acerca de la(s) persona(s) que lleva(n) adelante el proceso de implementación del servicio, como el tiempo aproximado en que estará activo el mismo.

SOLICITUD DE SERVICIOS DE SISTEMAS

TIPO DE SERVICIO

Cuenta Nueva: Mantenimiento: Dar de Baja:

Nombre Usuario : _____

Fecha de Solicitud: _____

Departamento : _____

Fecha de Recibido: _____

Sucursal : _____

Fecha de Trámite : _____

Use solo para mantenimientos: Indique servicios que tiene actualmente.

Nombre Usuario: _____

Menú de Datos: _____

Departamento : _____

Otro Servicio : _____

Nombre de Cuenta: _____

SERVICIOS SOLICITADOS

Tipo de Servicios	Marque X	Reservado para uso de Sistemas
Hardware		
Computador Portátil		
Escritorio		
Impresora Inyección		
Matricial		
Software		
Correo Interno:		Nombre de Cuenta :
Correo Externo		Dirección electrónica:
Acceso a Internet		Abierto: <input type="checkbox"/> Limitado: <input type="checkbox"/>
Acceso a Datos Menú		
Elite : _____		Nombre de Cuenta:
Nómina : _____		Nombre de Cuenta:
Granos : _____		Nombre de Cuenta:
Vehículos: _____		Nombre de Cuenta:
Otro : _____		
Comunicaciones:		
Extensión Teléfono		Número:
Celular:		Número:
Radio:		

Observación: _____

Solicitante	Ejecutado	Autorizado
Nombre: _____	Nombre: _____	Nombre: _____
_____ Jefe de Area	_____ Adminis trador	_____ Gerente de Sistemas

POLÍTICAS PARA LA ADQUISICIÓN DE UNA APLICACIÓN

Los requerimientos de información se determinan en base a la necesidad de la organización a través de cada departamento, una vez determinada la necesidad se analiza la factibilidad de desarrollar la aplicación con el equipo de sistemas que tiene la organización o adquirirla una aplicación que exista en el mercado que cumpla con los requerimientos de la organización haciéndose un análisis basado en costo beneficio para ello se aplica el siguiente procedimiento:

1. Se deben analizar varias soluciones de proveedores calificados cuyo productos cumpla con las exigencias mínimas establecidas.
2. Las alternativas deben ser evaluadas por un comité conformado por el gerente de sistemas, el jefe del área donde se utilizará la aplicación y un representante de auditoria, los términos de la negociación consultaría, cronograma de implementación, soporte técnico, forma de pago, etc, es responsabilidad del gerente de sistemas .la decisión final la tomará la gerencia general.
3. Considerando que la empresa requiere tener autonomía en el manejo de sus aplicaciones por ello cuenta con su propio equipo de sistemas, se recomienda incluir como requisito que el proveedor entregue los códigos fuentes de la aplicación, lo que permitirá a la empresa realizar sus modificaciones de acuerdo a la evolución del negocio.

PROCEDIMIENTO PARA EL DESARROLLO DE UNA APLICACIÓN

El gerente o jefe de una división o departamento plantea el requerimientos de información a la gerencia de sistemas se analiza la necesidad en conjunto entre el equipo de sistemas y los usuarios se determinan los objetivos, alcance, compatibilidad o interfase que será necesario para integrarlo al sistema central de la organización.

Una vez determinado los requerimientos específicos se elaboran los funcionales que servirán de base para el diseño de la aplicación por parte del equipo de sistemas.

Se procede con la elaboración del cronograma de implementación por parte del equipo de sistemas asignado al proyecto, se distribuye el trabajo de programación asignando funciones mediante la utilización de los formularios correspondientes que el departamento de sistemas utiliza para estos casos.

El proceso de desarrollo es supervisado y monitoreado por el gerente de sistemas quien deberá realizar mediciones de cumplimientos de acuerdo al cronograma y de acuerdo a las fechas de entrega por parte e cada programador.

PROCEDIMIENTO INTERNO DE SISTEMAS PARA LA MODIFICACIÓN DE UNA APLICACIÓN

La Gerencia de sistemas deberá asegurarse que, en caso de presentarse la necesidad de realizar modificaciones significativas a las aplicaciones actuales, dicho desarrollo se ajuste el estándar establecido en la organización, además de cumplir con todo lo recomendado en los procedimientos establecidos.

Se deben observar y respetar las normas y procedimientos que permitan mantener una estandarización y compatibilidad entre los diferentes sistemas de información que mantiene la empresa.

Las solicitudes deberán categorizar las prioridades y establecerse procedimientos específicos para manejar los casos urgentes. Los solicitantes de cambios deben permanecer informados acerca del estatus de su solicitud.

La Gerencia deberá asegurar que todas las requisiciones de cambios tanto internos como por parte de proveedores estén estandarizados y sujetos a procedimientos formales de administración de cambios.

1. El usuario a través del gerente o jefe departamental hace conocer el requerimiento al departamento de sistemas a través del formularios S1 "Requerimientos de Sistemas", en el cual se detallan todas las necesidades de información por parte del usuario.
2. El gerente de sistemas analiza el requerimiento si éste compromete la estructura de alguna aplicación o cambia los resultados de un proceso es puesto a consideración de la gerencia general para que autorice la viabilidad del pedido, de ser negado es devuelto al funcionario que solicitó la modificación manifestándole que no fue autorizado, en caso de ser procedente y estar justificado se procede a asignar el caso a un analista programador llenando previamente los formularios de acuerdo al procedimiento.
3. Si el cambio solicitado no tiene ningún impacto en la estructura de la base de datos o variación en el resultado de los reportes y consultas y se encuadra dentro de la información que está autorizada para ese departamento el gerente de sistemas da trámite al requerimiento, caso contrario lo somete a consideración de la gerencia general para su aprobación.
4. Una vez autorizado el nuevo requerimiento o modificación se determina el tiempo para su implementación que es dado a conocer al departamento solicitante procediéndose a llenar los formularios correspondientes para asignar el caso a un analista programador.
5. El gerente de sistemas asignará a cada analista programador o al equipo las modificaciones o proyecto a desarrollarse, determinándose previamente el tiempo aproximado para concluirlo.

6. Si es un mantenimiento se libera el código en el servidor de desarrollo donde el programador realizará las modificaciones y pruebas correspondiente una vez concluida las mismas procederá a documentar en el mismo código los cambios realizados conforme lo exige el standard de élite.
7. El programador notificará al gerente o al subgerente de sistemas quienes realizarán las revisiones y pruebas correspondientes así como la compilación del código para generar el objeto que será puesto en el servidor de producción.

Deberán implementarse procedimientos para asegurar que las modificaciones realizadas al software del sistema sean controladas de acuerdo con los procedimientos de administración de cambios de la organización.

AGRIPAC s.a.

Sistemas y Comunicaciones

Solicitud de requerimiento: Instrucciones de uso

El formulario S1, es el instrumento que utilizarán los usuarios del sistema para requerir del área de Sistemas y Comunicaciones, soluciones a los asuntos planteados en el mismo. Para lo cual, deberán escribir la siguiente información:

Empresa .- Nombre de la empresa;
Departamento.- Nombre del departamento;
Usuario .- Nombre del usuario;
Fecha .- Fecha de la solicitud.

Los casilleros ubicados en la parte superior derecha del formulario deberán marcarse, acorde a lo siguiente:

Nuevo Requerimiento.- Para implementar un nuevo programa dentro del menú asignado a cada usuario.

Modificación.- Para realizar cambios a cualquiera de los programas dentro del menú asignado a cada usuario. Si este casillero es marcado, deberá escribirse la letra o número que identifica a la opción o programa, como su nombre, a la derecha del título "Opción en el Menú".

Una vez que los datos de cabecera, han sido ingresados, los usuarios detallarán en forma amplia su requerimiento, en la caja denominada "Detalle del Requerimiento".

Los usuarios, en ningún caso, ingresarán información en la caja denominada "Para uso de Sistemas"; pero podrán anotar información adicional, a la derecha del título "Observ".

En toda solicitud, deberán constar 2 (dos) firmas, la primera, es la del usuario que solicita el requerimiento y la segunda, la de su inmediato superior.

Una vez aceptado un requerimiento por el área de Sistemas y Comunicaciones, se procederá a su asignación a uno de los Analistas, luego de lo cual, se notificará vía e-mail a los usuarios solicitantes, acerca de la(s) persona(s) que lleva(n) adelante el proceso de implementación, como el tiempo aproximado en que se será puesto en producción.

REQUERIMIENTOS DE SISTEMAS

Empresa : _____
Dpto : _____
Usuario : _____
Fecha : _____

Nuevo Requerimiento:
Modificación :
Prioridad (Baja-Media-Alta):
Opción en el Menú : _____

Detalle del Requerimiento

Para uso de Sistemas:

N. Requerimiento : _____
Módulo : _____
Fecha Recibido : _____ **Hora:** _____
Fecha Asignación: _____ **Hora:** _____
Analista Asignado: _____
Tiempo Estimado : _____ **Fecha de Entrega:** _____

Descripción técnica del Requerimiento:

SF-01

Observ: _____

Solicitante

Jefe Inmediato

Dpto. de Sistemas

AGRIPAC s.a.

Sistemas y Comunicaciones

Análisis Técnico: Instrucciones de uso

El formulario S2, es el instrumento que utilizan los analistas programadores para emitir un informe del análisis realizado ante un determinado requerimiento, en ese formulario se describe el módulo, proceso y códigos que se afectan con un determinado requerimiento Para lo cual, deberán escribir la siguiente información:

Analista	.- Nombre del analista;
Requerimiento	.- Tipo de Requerimiento;
Solicitante	.- Nombre del usuario;
Fecha	.- Fecha de la solicitud.
Hora	.- Hora de la solicitud
Area	.- Area que realiza el requerimiento.

Como todos los formularios se lleva un cronológico que permite llevar un consecutivo y relacionarlo con los demás formularios que corresponden al mismo caso que se origina con el requerimiento de usuario.

En la descripción se registra de manera detallada el resultado del análisis realizado por el analista responsable de atender este requerimiento, se deja constancia de las tablas, módulos, aplicaciones y códigos que se ven afectados por la modificación o por el nuevo requerimiento.

En toda solicitud, deberán constar 2 (dos) firmas, la primera, es la del analista responsable requerimiento y la segunda, la firma del gerente de sistemas quien da su aprobación, observación o rechazo al análisis.

AGRIPAC s.a.

Sistemas y Comunicaciones

Ficha técnica de Modificaciones: Instrucciones de uso

El formulario S3, es un instrumento para uso interno del departamento de sistemas que permite llevar el control del desarrollo de los nuevos requerimientos y las modificaciones que están en proceso de desarrollo, así como el trabajo encargado a cada analista programador, las prioridades, las fechas de cumplimiento, los códigos que tienen que ser modificados y la fecha de entrega del proyecto que debe coincidir con la fecha dada a los usuarios para concluir con el requerimiento y ponerlo en producción una vez que se cumpla con todas las fases que obligatoriamente se deben ejecutar a todos los procesos de desarrollo, los datos que se registran en este formulario son los siguientes.

Fecha .- Fecha de asignación al analista;
Compañía .- Nombre de la empresa;
Proceso .- El proceso afectado;
Módulo .- El módulo al que corresponde el requerimiento;
Prioridad .- La prioridad asignada al requerimiento;
Responsable Proyecto .- El analista responsable;
Fecha de Entrega .- La fecha máxima de entrega;
Cumplimiento .- El cumplimiento en la entrega.

Los casilleros de la parte inferior permiten registrar los detalles técnicos del requerimiento en el siguiente orden.

En el primer casillero se registra el o los códigos que deben ser modificados.

En Detalle de modificaciones, se deja constancia al cambio en sí que se le está haciendo al código lo que permite llevar una bitácora sobre los cambios realizados a un determinado código o programa fuente.

Analista Responsable, se registra el nombre del o los analistas responsable(s) dependiendo el requerimiento se dan casos en que un requerimiento afecta a varios programas o códigos lo que hace necesario la participación de más de un programador.

Se determina un tiempo estimado en horas para realizar los cambios o modificaciones por códigos esto permite llevar un control de las tareas asignadas a cada programador en relación a las horas trabajadas.

En el siguiente casillero se describe la fecha que se determinó para que sea concluido el trabajo por parte del programador.

El casillero siguiente permite registrar la fecha real de terminación del trabajo por parte del programador.

EL siguiente casillero permite determinar el cumplimiento entre la fecha estimada para la terminación del trabajo y la fecha real.

En la parte inferior se ponen las observaciones o comentarios que justifiquen cualquier novedad referente a al requerimiento o motivo de variación de parámetros, fechas o cualquier otro motivo referente a este tópico.

Finalmente se deja constancia de la asignación y aceptación del trabajo mediante la firma del analista responsable y el gerente de sistemas.

FICHA TECNICA DE MODIFICACIONES

FECHA :	PRIORIDAD :
COMPAÑÍA :	RESPONSABLE PROYECTO :
PROCESO :	FECHA MAXIMA ENTREGA :
MODULO :	CUMPLIMIENTO :

DESCRIPCION

Código (N-M)	Detalle de Modificaciones	Analista Responsable	Tiempo Estimado Horas	Fecha Entrega Estimada	Fecha Entrega Real	Cumplimiento

FS-03

Observación: _____

Analista Responsable

Gerencia de Sistemas

AGRIPAC s.a.

Sistemas y Comunicaciones

Prueba de Requerimientos y Modificaciones: Instrucciones de uso

El formulario S4, es un instrumento para uso interno del departamento de sistemas que permite realizar las pruebas en el ambiente de desarrollo y cuando éstas han concluido poder hacerlas con la participación del usuario para tener su aceptación o no satisfacción, lo que retroalimenta el proceso para que el programador corrija o incorpore lo planteado por el usuario siempre y cuando haya sido estipulado en el requerimiento original que está contemplado en el formulario S1.

En caso de estar de acuerdo el usuario con la modificación o con el nuevo requerimiento se comunica al responsable del ambiente de producción quien procede a revisar la modificación en el código y además debe tomar las medidas correspondientes para garantizar que el código no haya sido modificado en las demás instrucciones ni que se haya incluido ninguna instrucción diferente a la solicitada por el usuario. Una vez revisado cuidadosamente es pasado a producción al mismo tiempo es comunicado a la gerencia de sistema quien firma y comunica a los usuarios que está listo el requerimiento para que procedan a utilizarlo.

Se procede a llenar todos los casilleros con la información correspondiente incluyendo las firmas del usuario para dejar constancia de su aceptación en cuanto al funcionamiento y de que el cambio se ajusta al requerimiento, así como la firma del responsable de producción y del gerente de sistemas.

En la parte inferior se detallan las observaciones o comentarios que se consideren necesario.

Finalmente se deja constancia de la asignación y aceptación del trabajo mediante la firma del analista responsable y el gerente de sistemas.

PRUEBA DE REQUERIMIENTOS Y MODIFICACIONES

Compañía :		Fecha Solicitud :	
Módulo :		Prioridad :	
Proceso :		Cumplimiento :	
Nombre Usuario :		Analista Responsable:	

DESCRIPCION

Código (N-M)	Detalle de la Prueba	Fecha y Hora de la Prueba	Firma Aceptación Usuario	Autorización a Producción

SF-04

Observación: _____

Analista Responsable-----
Gerente de Sistemas

AGRIPAC s.a.
Sistemas y Comunicaciones

Control de Requerimientos y Modificaciones:
Instrucciones de uso

El formulario S5, es un instrumento para uso interno del departamento de sistemas que permite llevar el control del desarrollo de los nuevos requerimientos y las modificaciones que están en proceso de desarrollo, así como el trabajo encargado a cada analista programador, las prioridades, las fechas de cumplimiento, los códigos que tienen que ser modificados y la fecha de entrega del proyecto que debe coincidir con la fecha dada a los usuarios para concluir con el requerimiento y ponerlo en producción una vez que se cumpla con todas las fases que obligatoriamente se deben ejecutar a todos los procesos de desarrollo, los datos que se registran en este formulario son los siguientes.

Fecha del Requerimiento.

Número del Requerimiento

Módulo Afectado

Código o nombre del Programa a Modificarse.

Detalle de la Modificación

Prioridad de la Modificación

Tiempo estimado(en horas) para realizar el trabajo.

Analista Programador responsable.

Fecha de entrega del trabajo por parte del programador.

El casilleros de la parte inferior izquierda permiten registrar las novedades que se presenten durante el proceso de desarrollo por parte del programador.

El casillero de la parte inferior derecha la gerencia de sistemas o el responsable del ambiente de producción registren cualquier información que sea necesaria durante el desarrollo del requerimiento.

Finalmente se deja constancia mediante la firma del analista responsable y el gerente de sistemas.

CONTROL DE REQUERIMIENTOS Y MODIFICACIONES

Ítem N.	Módulo Afectado	Código Programa	Detalle de Modificaciones	Prioridad	Tiempo Estimado	Analista Responsable	Fecha de Entrega

SF-05

Observaciones durante el Proceso de Desarrollo

Observaciones de la Gerencia de Sistemas