ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada (MSIA)

"DESARROLLO E IMPLEMENTACIÓN DE UN PLAN DE CONTINUIDAD DE NEGOCIO Y DE RECUPERACION DE DESASTRE EN LA EMPRESA AGRIPAC S. A."

TRABAJO DE TITULACIÓN

Previo a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

CESAR BOLIVAR VALLEJO PERALTA

GUAYAQUIL - ECUADOR

AÑO: 2015

AGRADECIMIENTO

Quiero agradecerle a mi Dios, a la Santísima Virgen y a todas las personas que de forma directa e indirecta me apoyaron para lograr este importante objetivo, un agradecimiento especial a mi amada esposa y a mis queridos hijos quienes me motivaron y fueron mis promotores para concluir esta tesis de titulación que me permitirá cerrar de forma exitosa mi carrera profesional y personal.

Agradezco también a esa gran organización “Agripac S.A.” y muy en particular a su Presidente Ing. Colin Armstrong por su apoyo para la elaboración y la inmediata ejecución de este importante proyecto, así como también por la confianza y su respaldo brindado durante los 35 años como gerente del área de tecnología.

DEDICATORIA

Dedico esta tesis a mi amada esposa y a mis queridos hijos quienes me motivaron para que concluya este trabajo pendiente y terminar exitosamente uno de los objetivos más importantes de mi vida profesional y personal, ellos siempre fueron mi inspiración, la razón para fijarme grandes objetivos y luchar hasta alcanzarlos, hoy me siento orgulloso de verlos realizados como personas de bien y profesionales exitosos que se siguen preparando para crecer en su especialidad y que además están consciente que los grandes objetivos no son fáciles de lograr pero se los alcanza con dedicación, sacrificios, honestidad y una profunda fe en Dios.

TRIBUNAL DE SUSTENTACIÓN

MSIG. Lenín Freire C.

Coordinador de Maestría

MG. Fabián Barboza

Director del Proyecto de Graduación

MG. Albert Espinal S.

Miembro del Tribunal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual del mismo a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

_____

Ing. César B. Vallejo Peralta.

RESUMEN

Este proyecto es altamente importante para Agripac, porque no solamente garantiza la continuidad de sus procesos críticos sino que también contribuye a generar confianza en sus cliente, empleados, proveedores, sistema financiero, Organismos de Control y accionistas, fortaleciendo así la imagen de esta prestigiosa empresa.

En cada uno de los capítulos se describen detalladamente las secciones y actividades que lo conforman permitiendo así una mejor comprensión de este importante proyecto.

En el capítulo 1, se detallan los antecedentes, se describe el problema y la solución del mismo, igualmente se plantean los objetivos generales y específicos que se deben alcanzar con la implementación de este proyecto.

El capítulo 2 describe el marco teórico [14] que brinda una comprensión objetiva de la organización y del problema, se describen los principios de

seguridad informática y determina los requisitos mínimos para poder implementar un plan de continuidad de negocio y recuperación de desastre.

En el capítulo 3, se expone la situación actual así como el levantamiento de información, el ambiente de sistemas así como la administración y control de tecnología de información, los roles y responsabilidades, la infraestructura técnica y aplicaciones.

En el capítulo 4, se realizó el análisis del diseño del Plan de Continuidad de Negocio y de Recuperación de Desastre, se definió una matriz de vulnerabilidades y los criterios para la declaratoria de contingencia, con cada uno de los posibles escenarios.

En el capítulo 5 se determinan las fases del plan de acción, la estructura organizacional del plan de contingencia, el Comité de Contingencia, los equipos de trabajo y sus responsabilidades así como las estrategias y alternativas de recuperación.

En el capítulo 6 se describen las diferentes pruebas que deben realizarse para garantizar que el plan de continuidad funciona de acuerdo a lo previsto en cada una de las fases del proyecto, entre las principales pruebas tenemos:

Pruebas de conectividad con el data center del proveedor, pruebas de configuración de routers, pruebas de puntos de red en el centro alterno, pruebas de desvíos de enlaces de las plantas y puntos de ventas hacia el data center de la nube, pruebas de acceso al servidor en la nube (cloud).

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

AD	Active Directory - Directorio Activo de Microsoft.
BIA	Business Impact Analysis – Análisis de impacto al negocio
BCP	Business Continuity Plan – Plan de continuidad del negocio
CNT	Corporación Nacional de Telecomunicaciones
DMZ	Demilitarized zone – Zona desmilitarizada o red perimetral es una zona segura que se ubica entre la red interna y una red externa
DRP	Disaster Recovery Plan – Plan de recuperación ante desastres
ERP	Enterprise Resource Planning. Software de gestión integrada
HTTP	Hypertext Transfer Protocol – Protocolo de Transferencia de Hipertexto
HTTPS	Hypertext Transfer Protocol Secure - Protocolo Seguro de Transferencia de Hipertexto

ISO	International Organization for Standardization - Organización Internacional de Normalización
NAT	Network Address Translation – Traducción de direcciones de red.
QOS	Quality of Service – Calidad de Servicio
RAID	Redundant Array of Inexpensive Disks – Conjunto redundante de discos independientes.
SAP	Systems, Applications and Products – Sistema informático basado en módulos integrados.
TIC	Tecnología de Información y Comunicación.
TIER	Norma que indica el nivel de fiabilidad de un centro de datos asociados a cuatro niveles de disponibilidad definidos
UTM	Unified Threat Management – Gestión Unificada de Amenazas
WAF	Web Application Firewall

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

AGRIPAC S. A. Es una organización comercial que importa, formula, distribuye y comercializa productos para la agroindustria, es muy reconocida en todo el país, cuenta con 5 plantas y 170 sucursales propias en todas las provincias del país, tiene 1200 empleados y sus ventas son de 300 millones aproximadamente, cuenta con varias líneas de negocios, todas están integradas y se apoyan fuertemente en la tecnología lo que les permite manejar de manera eficiente sus operaciones, entre las más destacadas tenemos:

UNIDADES DE NEGOCIO:

Oficina Matriz (180 usuarios)

5 Plantas de Producción: Pascuales – Balanfarina – Laquinsa - Agrigrain y Quito (180 usuarios)

25 Sub-centros de Abastecimiento

170 Puntos de Ventas Remotos

Se establece el contexto para la lectura de la guía del Plan de Continuidad del Negocio y de Recuperación de Desastre, esta guía también nos da una pausa para reflexionar sobre la necesidad que tiene la empresa de contar con un Plan de Contingencia que le permita recuperarse de un desastre en el menor tiempo

posible, sin que se afecten sus principales procesos considerados como críticos ni su imagen.

Cuando una organización se embarca en un Plan de Continuidad de Negocio y de Recuperación de Desastre [12] debe implementar los siguientes pasos claves:

- Desarrollar la política del Plan de Continuidad de Negocio y de Recuperación de Desastre.
- Alinear la política con la estrategia, objetivos y cultura organizacionales.
- Decidir sobre el alcance del Plan de Continuidad de Negocio y de Recuperación de Desastre.
- Entender que un Plan de Continuidad de Negocio y de Recuperación de Desastre, no es un proyecto de tecnología sino un programa continuo de toda la organización que debe ser difundido, entendido, probado y medido.

CAPÍTULO 1

GENERALIDADES

1.1 ANTECEDENTES

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 acuacultura, que cuenta actualmente con 170 sucursales ubicadas en las diferentes provincias del país.

La 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.

Cuenta con 170 almacenes y personal técnico y comercial de primer nivel a lo largo de todo el país lo que garantiza una entrega oportuna y asesoramiento permanente a los clientes. Además, la calidad de nuestros productos permite 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. Es el principal proveedor 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 Micro elementos.

- **La División CONSUMO de AGRIPAC**, ofrece una línea de alimentos para mascotas (perros y gatos) de alta calidad, igualmente una amplia línea de prestigiosos productos para el control de plagas tanto a nivel de

hogares (Dragón, Klerat, etc.) como de industrias siendo líderes en esta línea 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.

Produce las reconocidas marcas de alimento para mascotas BUEN CAN y MICHU las mismas que en los últimos tres años por su alta calidad se han posesionado como la segunda y primera en el mercado nacional, y se las distribuye a través de su propia cadena de distribución.

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 45 Toneladas 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 especias menores.

La empresa tiene una participación en el mercado que la consolida como una de las empresas más importante del país, su volumen de transacciones es aproximadamente de 6 millones mensuales. Cuenta en su estructura organizacional con 1100 empleados a nivel nacional y su facturación está estimada en 290 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 veinte 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 garanticen la continuidad del negocio.

El Plan de Continuidad de Negocios y de Recuperación de Desastre está enfocado en reducir los riesgos que ocasionen problemas en las

operaciones normales de la 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.

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.

1.2 DESCRIPCIÓN DEL PROBLEMA

Agripac S.A. es un Grupo Corporativo que importa, fabrica, distribuye y comercializa productos para la agroindustria, entre sus principales líneas de negocios están la Agrícola, Acuacultura, Avícola, Ganadera, alimento para mascotas, Servicio de Fumigación con aviones propios, cuenta con cinco plantas de producción y 170 sucursales ubicadas en las diferentes provincias del país, tiene 1200 empleados, su facturación aproximada es de 290 millones de dólares anuales, es una empresa líder en su mercado y está ubicada entre las 50 empresas más importantes del país.

La organización maneja todas sus operaciones de forma centralizada en sus oficinas matriz ubicada en Guayaquil, para ello cuenta con un sistema de información integrado “ERP-SAP” que le brinda información en línea la misma que sirve de base para tomar todas las decisiones, todas las plantas así como los puntos de ventas están conectados al centro de cómputo de la oficina matriz mediante enlaces de comunicaciones "punto a punto".

La empresa cuenta con un servidor de respaldos que está ubicado en el mismo centro de cómputo que le permite reaccionar ante incidentes o fallas menores, pero la preocupación de la gerencia de TI es porque la empresa no cuenta con un Plan de Contingencia que le permita garantizar la continuidad de las operaciones o reactivar los procesos críticos en caso de presentarse un incidente mayor considerado como “desastre” ejemplo: incendio, terremoto, atentado terrorista, etc., lo que implica un riesgo latente muy alto, porque para restaurar su sistema de información se requiere un tiempo mayor que el Máximo Periodo Tolerable de Interrupción (MPTI) de la empresa, lo que pondría en inminente riesgo la continuidad del negocio y la existencia misma de la empresa.

Principales Problemas:

- No se cuenta con una contingencia de los servidores de producción fuera de las instalaciones de la empresa lo que implica un alto riesgo para la existencia misma de la organización.

- La empresa no cuenta con un Plan de Recuperación de Desastre Tecnológico que le permita reactivar sus operaciones después dentro de un máximo período tolerable, después de un incidente mayor considerado como desastre, como puede ser; incendio, terremoto, atentado terrorista, etc.

- No se cumple con las exigencias de los Organismos de Control respecto a contar con un plan de Continuidad del Negocio.

1.3 SOLUCIÓN PROPUESTA

La propuesta consiste en implementar un Plan de Continuidad de Negocio y de Recuperación de Desastres (DRP), que incluye migrar a un Data Center a la nube (Cloud) un respaldo o backup del servidor de Producción y del servidor de Análisis de Datos, los mismos que se actualizarían en línea, lo que permitirá contar con una réplica en tiempo real para garantizar la continuidad de las operaciones en caso de una eventual destrucción/daño temporal o permanente de las instalaciones que se encuentran ubicados en el centro de cómputo. También considera

implementar un centro alterno en la planta Balanfarina que se encuentra ubicada en el Km 6 vía Durán Tambo, el mismo que servirá como centro de operaciones durante la activación del Plan de Continuidad de Negocio y de Recuperación de Desastre.

Para la implementación del Plan de Continuidad de Negocio y de Recuperación de Desastre no solamente se debe involucrar a personal de sistemas sino que también se requiere la participación de personal claves de las diferentes áreas de la organización.

Beneficios de la solución planteada:

- Garantizar la continuidad de las operaciones de los servicios críticos de la empresa luego de la materialización de un desastre natural o provocado que afecte la infraestructura del centro de datos que está en la oficina matriz.

- Precautelar la información que es el activo más preciado de la organización.

- Cumplir con lo dispuesto por los Organismos de Control, sistema financiero y proveedores que exigen que la empresa cuente con un Plan de Continuidad de Negocio.

- Precautelar la imagen de la empresa ante clientes y proveedores.

- Brindar tranquilidad a los accionistas porque se garantiza la supervivencia de la empresa después de un incidente mayor o desastre que impida el funcionamiento del actual centro de cómputo.

Para una mejor exposición y comprensión de la solución planteada se la ha dividido en dos fases estas son:

Infraestructura Actual

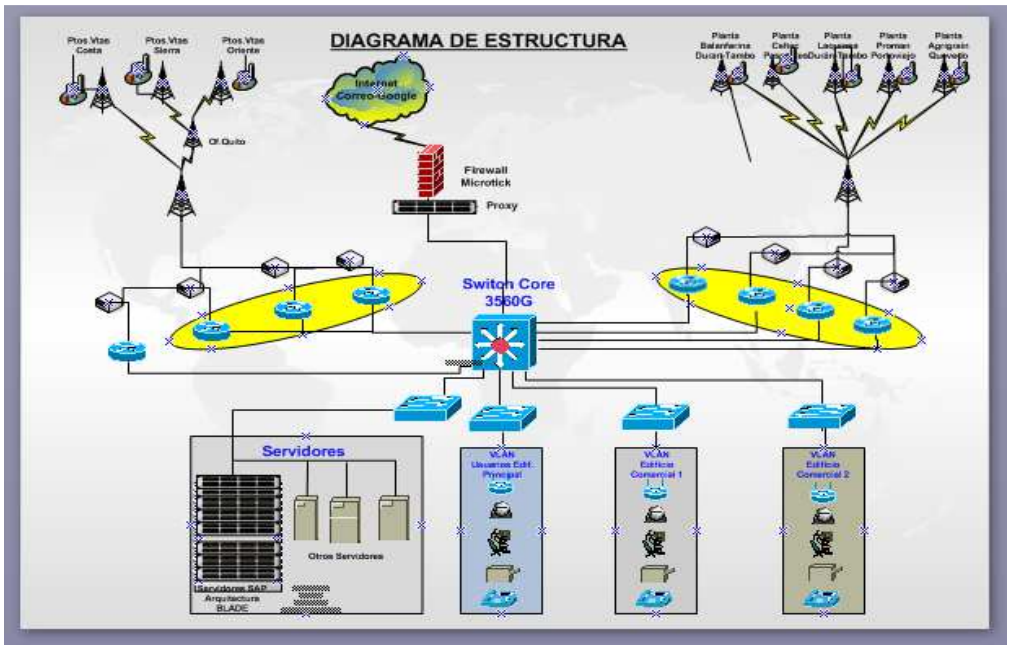


Figura 1.1 Infraestructura de red actual

Infraestructura Propuesta

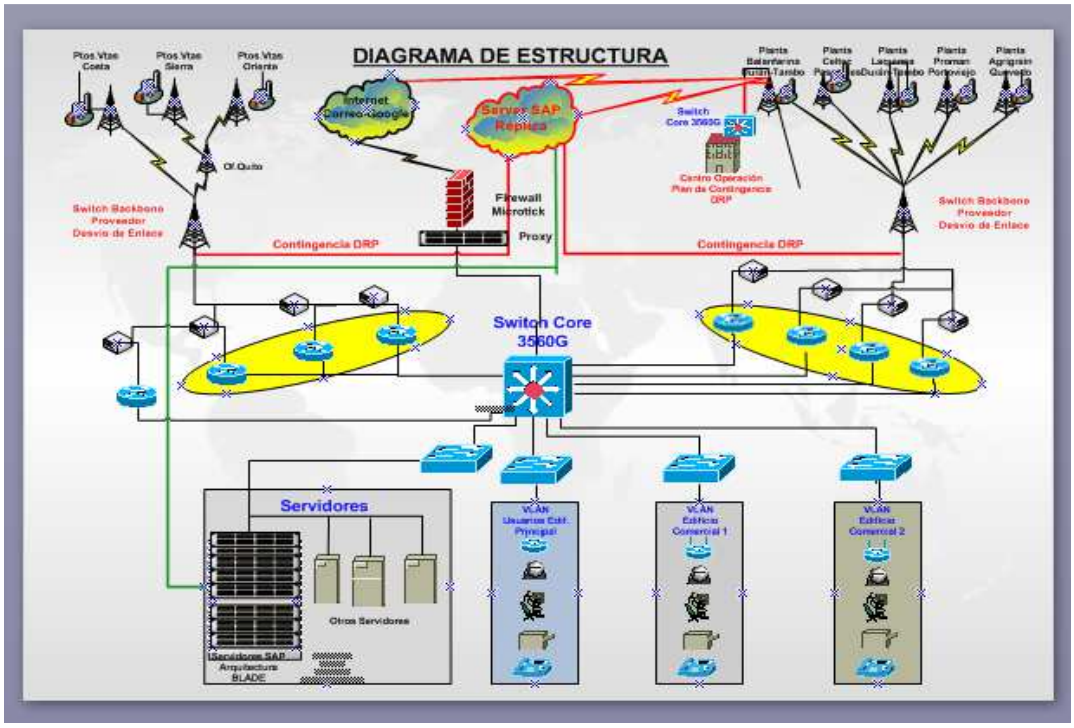


Figura 1.2 Infraestructura de red propuesta

Fase Técnica:

Incluye las siguientes actividades:

A. Seleccionar Proveedor de Servicio en la Nube.

B. Dimensionar requerimientos de hardware, software y medios de conectividad.

C. Configuración y migración de servidores

D. Instalación y Configuración de equipos en backbone del proveedor de comunicaciones para poder desviar los enlaces hacia el Centro de Cómputo de Emergencia desde donde se activará el BCP-DRP.

E. Habilitación de instalaciones físicas para el Centro de Cómputo de Emergencia en la planta ubicada en el Km. 6 vía Durán Tambo.

F. Instalación y Configuración de equipos de comunicaciones en el Centro de Cómputo de Emergencia.

Fase Operativa:

A. Conformar Comité del Plan de Contingencia y Funciones de sus miembros.

B. Determinar ubicación y habilitación del Centro alterno de operaciones

C. Realizar un análisis de riesgos enfocado a los procesos para determinar los procesos críticos.

D. Identificar y Priorizar los elementos críticos por servicio, necesarios para operar durante la contingencia (recursos tecnológicos, de información, humanos, materiales, etc.).

D. Determinar los escenarios de contingencia.

E. Organizar los equipos de trabajo para operar en modalidad de contingencia

1.4 OBJETIVO GENERAL

Implementación de un Plan de Continuidad de Negocio s y Recuperación de Desastre para el Grupo Corporativo AGRIPAC S. A.

1.5 OBJETIVOS ESPECÍFICOS

1 Garantizar la continuidad de las operaciones estratégicas de la empresa inmediatamente después de cualquier incidente considerado como desastre.

2 Mantener el control de los servicios de TI en modalidad de Contingencia, los mismos que estarán a cargo del gerente de Tecnología e Información.

3 Organizar los grupos de usuarios responsables de las operaciones en contingencia, la coordinación y control y las actividades necesarias para normalizar las operaciones críticas así como los servicios una vez pasada la contingencia.

4 Identificar y documentar los procesos, actividades y procedimientos necesarios para las operaciones en contingencia y la posterior normalización de los mismos.

5 Identificar, dimensionar, presupuestar y organizar los recursos necesarios para las operaciones de los procesos críticos en contingencia en un site provisional.

1.6 METODOLOGÍA

Dentro de la Metodología se ha considerado los objetivos de ISO 22301 [4] relacionados directamente a la Continuidad de los Negocios y Recuperación de Desastre, el proyecto describe los pasos necesarios [15] para poder asegurar que las Operaciones consideradas estratégicas o críticas puedan ser reactivas en poco tiempo después de ser interrumpidas por la materialización de cualquier incidente mayor que sea considerado como desastre.

Cada proceso soportado fuertemente por Tecnología debe ser considerado para ser analizado y se deben determinar las vulnerabilidades así como el nivel de riesgos y su impacto en el negocio.

Las posibles fallas deben ser identificadas y en base a ellas se debe establecer un tiempo máximo de recuperación y la probabilidad de que éstas se presenten.

CAPÍTULO 2

MARCO TEÓRICO

2.1 PLAN DE CONTINUIDAD DE NEGOCIO Y DE RECUPERACIÓN DE DESASTRE

El Plan de Continuidad de Negocio y de Recuperación de Desastre está enfocado en reducir los riesgos que ocasionen problemas en las operaciones normales de la organización para salvaguardar que el nivel de impacto de estos posibles incidentes no ocasione la inoperatividad de los procesos considerados críticos e identificar los recursos alternativos.

El Plan de Continuidad del Negocio y de Recuperación de Desastre está diseñado para ser aplicado sobre una posible amenaza de desastre para

la empresa Agripac S.A considerando 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 está ubicado 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.

Uno de los problemas que normalmente se debe superar para la implementación de un Plan de Continuidad de Negocio y de Recuperación de Desastre [1] es el convencer a la alta gerencia sobre la justificación de hacer una inversión significativa en algo que probablemente nunca suceda, de allí la importancia de realizar un Análisis de Impacto en el Negocio (BIA) que es un proceso de gestión integral que identifica potenciales impactos de una amenaza a la organización y provee una capacidad de respuesta efectiva para proteger los intereses de los inversionistas, clientes, empleados y de la imagen de la empresa ante la

ocurrencia de un desastre que interrumpa las operaciones por un largo tiempo, lo que además agrega valor, esto permitirá justificar plenamente la implementación del Plan de Continuidad de Negocio y de Recuperación de Desastre. [2]

Figura 2.1 Fases del Plan de BCP

2.2 PLAN DE RECUPERACIÓN DE DESASTRE

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.

Otros aspectos importantes que deben tenerse en cuenta al elaborar un Plan de Recuperación de Desastre son los siguientes:

• BCP/PRD no es solo una respuesta, es la capacidad de una empresa para hacer frente a los impactos de un medio incierto.

• BCP/PRD no es solo apagar fuego, es entender que pueden existir riesgos y establecer estrategias si pensamos que vamos hacia ello.

• BCP/PRD no es solo tener planes súper elaborados, es tener planes que se ajusten a la naturaleza de su negocio.

• BCP/PRD no está anexado al negocio, debe estar incorporado íntegramente con el gerenciamiento del proceso y del riesgo en general como parte de un buen gerenciamiento del negocio.

La realización del BCP/PRD en la organización traerá grandes ventajas como por ejemplo:

• Administrar la continuidad del negocio.

• Resistencia del negocio ante interrupciones.

• Detectar los aspectos vulnerables y las posibles causas.

• Protege y asegura la imagen de la empresa.

• Abre nuevas oportunidades de mercado y ayuda a ganar nuevos negocios.

• Aumenta la disponibilidad del negocio.

2.3 NORMATIVAS

Para la implementación del Plan de Continuidad de Negocio y de Recuperación de Desastre tomamos como base la Norma ISO/IEC 22301[3] para garantizar la Gestión de Continuidad de Negocio [13] y Recuperación de Desastre, esta Norma [6] indica los requisitos así como los pasos a seguir para la implementación de un Plan de Continuidad de Negocio orientado a proteger la supervivencia de la empresa ante la materialización de incidentes mayores considerados desastres que puedan provocar la interrupción de los procesos considerados críticos, reducir la probabilidad de que se produzcan, minimizar su impacto así como la recuperación en un tiempo máximo estimado de los procesos críticos de la empresa [10].

4 Figura 2.2 Procesos que incluye la ISO 22301

Ventajas de la Norma ISO 22301: Gestión de la Continuidad de Negocio [5]

- Identificar y dimensionar los riesgos actuales y futuras para su organización.
- Medir y minimizar el impacto de esos riesgos en caso de materializarse.
- Capacidad para activar los procesos críticos del negocio en un tiempo considerado máximo luego de ocurrir un evento considerado desastre.
- Minimizar el tiempo de interrupción tras cualquier incidencia y mejorar el tiempo de recuperación

- Precautelar la permanencia de la empresa en el tiempo.

2.4 SEGURIDAD DE INFORMACIÓN.

Agripac mantiene un sistema de información integrado y en línea, por el alto volumen de transacciones que maneja requiere de un robusto sistema de Seguridad que le permita procesar y garantizar la seguridad, disponibilidad y confidencialidad de la información para la toma de sus decisiones.

El aplicativo integrado que maneja el CORE del negocio es SAP el mismo que incorpora las mejores prácticas de accesos, segregación de funciones y lleva una amplia auditoría que permite garantizar la trazabilidad de todos los procesos.

La red de datos está segmentada y posee redundancia para garantizar la disponibilidad de acceso tanto para los usuarios locales como a los remotos, La seguridad y control de accesos se las realiza con un UTM (Gestión Unificada de Amenazas) Appliance Cyber Roam de gama alta (Firewall-Proxy-Security) y routers Cisco Catalyst de la serie 3750 que permite manejar los altos volúmenes de transacciones que genera la empresa.

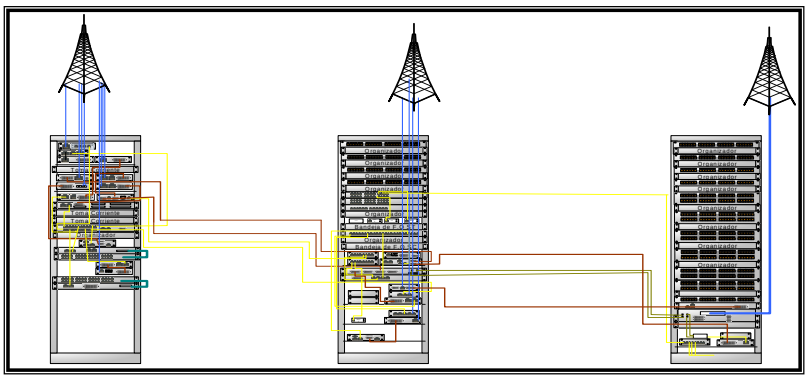


Figura 2.3 Estructura de la red

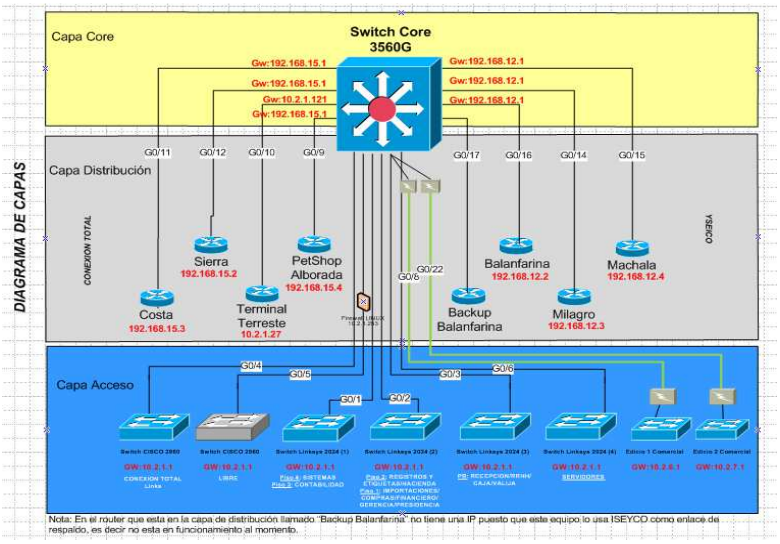


Figura 2.4 Diagrama de Capas de red

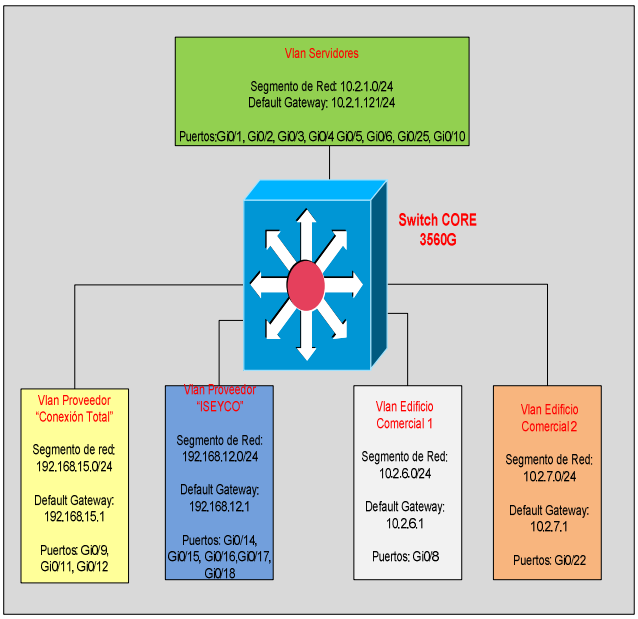


Figura 2.5 Diagrama de VLans

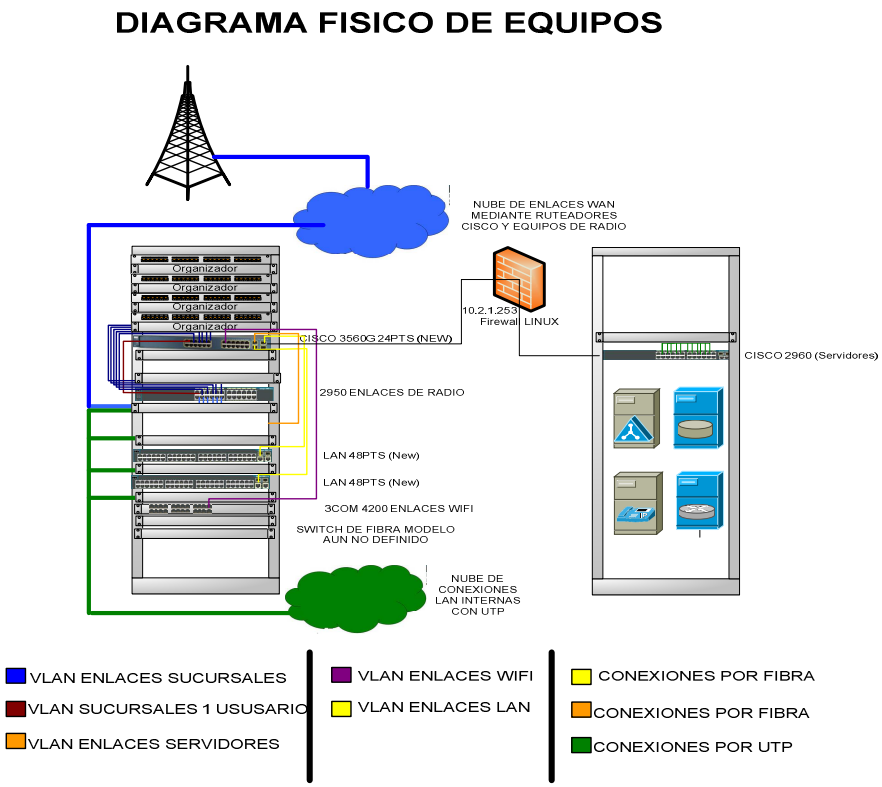


Figura 2.6 Diagrama físico de equipos

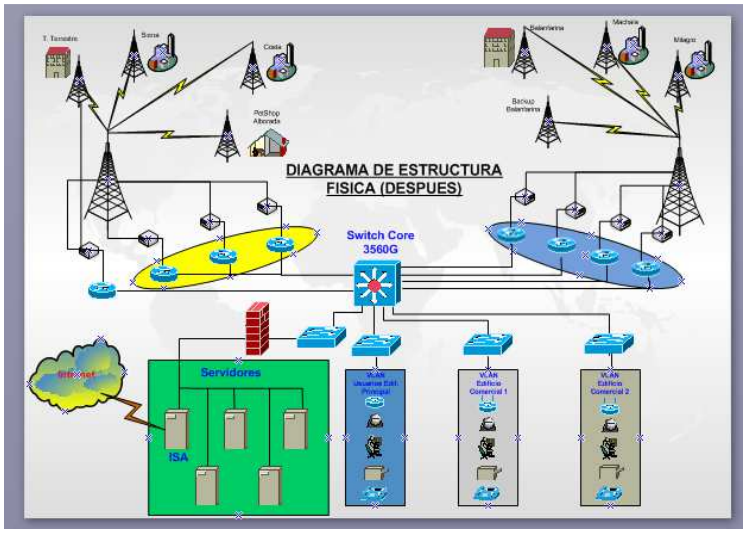


Figura 2.7 Diagrama de Estructura Física propuesta

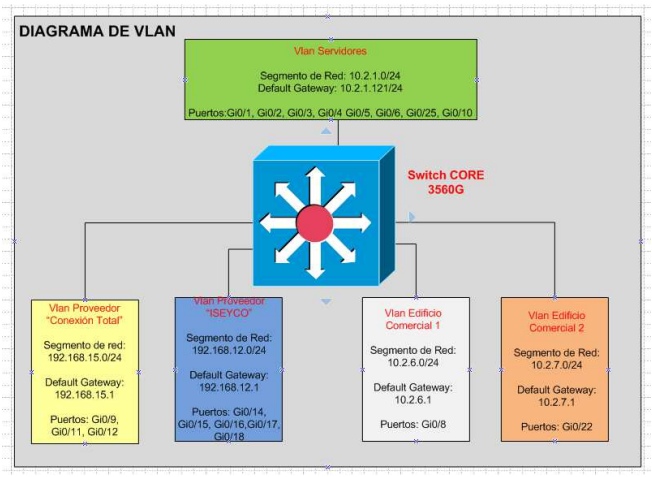


Figura 2.8 Diagrama de VLan propuesta

2.5 INFRAESTRUCTURA DE TI

La organización cuenta con una infraestructura de TI robusta conformada por una red de categoría 6A la misma que está segmentada y a la que se conectan 800 usuarios (180 locales y 620 remotos) cuenta con 170 punto a punto ubicados en todas las provincias del país y 5 plantas de producción, los usuarios remotos están conectados en línea mediante enlaces de radio punto a punto.

La infraestructura de servidores es de arquitectura x86 BLADE actualmente posee 20 servidores que soportan diferentes aplicativos y procesos de la organización.

Servidores:

Tabla 1 Tabla de Servidores para Aplicativo SAP

Nombre Servidor	Descripción Servicio Presta	N. Proc.	Procesador	Memo-ria	Discos	Sistema Operativo Ver.
agripsap01	- CUPS Servidor de Impresión Puntos	1	Intel(R) Xeon(R) CPU E5502 @ 1.87GHz	24 GB	2 Disk SAS 146 GB	Red Hat Enterprise Linux Server re-lease 5.4 (Tikanga)
agripsap02	Solution Manager (SOLMAN)	1	Intel(R) Xeon(R) CPU E5502 @ 1.87GHz	22 GB	2 Disk SAS 146 GB	Red Hat Enterprise Linux Server re-lease 5.4 (Tikanga)
agripsap03	Desarrollo ERP (DEV) Calidad ERP(QAS)	2	Intel(R) Xeon(R) CPU E7450 @ 2.40GHz	49 GB	2 Disk SAS 146 GB	Red Hat Enterprise Linux Server re-lease 5.8 (Tikanga)
agripsap04	Análisis de Datos Desarrollo BW (DEW) Calidad BW (QBW)	1	Intel(R) Xeon(R) CPU E5520 @ 2.27GHz	132 GB	2 Disk SAS 146 GB	Red Hat Enterprise Linux Server re-lease 5.4 (Tikanga)
agripsap05	Producción ERP (PRD) ORACLE 10.2.0.4	4	Intel(R) Xeon(R) CPU E5-2670 v2 @ 2.50GHz	256 GB	4 Disk SSD 200 GB	Red Hat Enterprise Linux Server re-lease 5.8 (Tikanga)
agripsap06	Análisis de Datos Producción BW (PRW)	2	Intel(R) Xeon(R) CPU E5-2670 v2 @ 2.50GHz	132 GB	2 Disk SAS 146 GB	Red Hat Enterprise Linux Server re-lease 5.8 (Tikanga)
agripsap08	Replica de Producción Servidor de Impresión CUPS	2	Intel(R) Xeon(R) CPU E5520 @ 2.27GHz	256 GB	4 Disk SAS 400 GB	Red Hat Enterprise Linux Server re-lease 5.8(Tikanga)

STORAGE

Tabla 2 Información de Storage Hitachi

Marca-Modelo	Capacidad	N. DISCOS	Sist. Operativo Base de datos
HITACHI HUS 110	39 TB	27 x 200 GB SSD 56 x 600 GB SAS	Linux Ret Hat Oracle v. 10.5
HITACHI AMS 2100	19.8 TB	44 x 450 GB SAS	Linux Ret Hat Oracle v.10.5

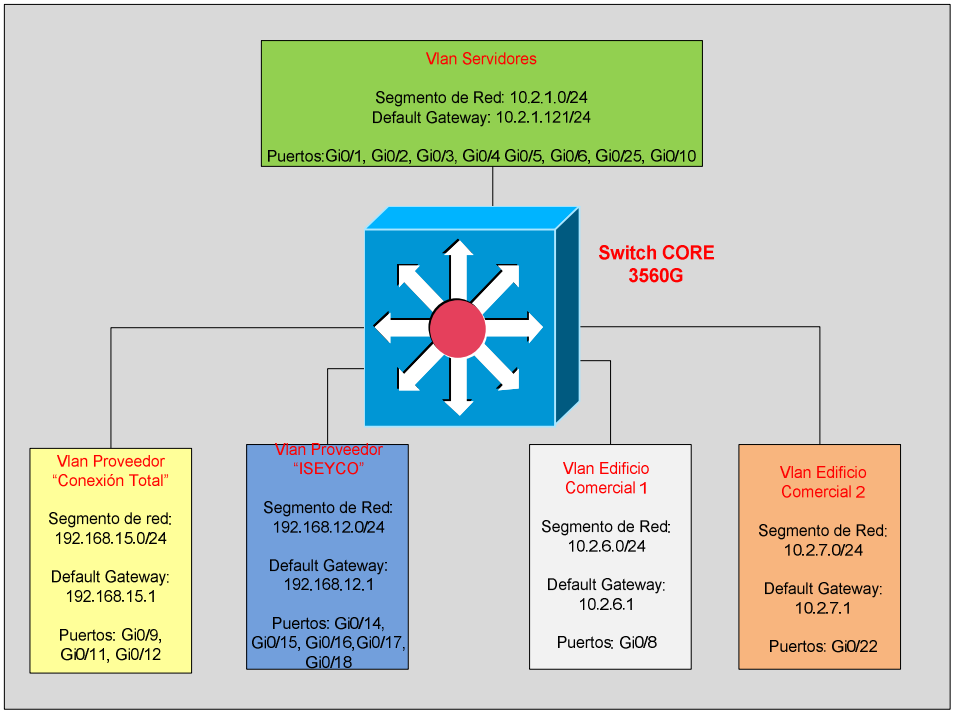


Figura 2.9 Configuración de VLAN's en Switch Core

El sistema operativo es Linux Ret Hat para SAP con base de Datos Oracle.

Las estaciones de trabajo utilizan Linux Ubuntu, los ejecutivos y Directores utilizan Windows.

La información de todas las áreas de la empresa se la maneja de forma centralizada con el aplicativo integrado SAP el mismo que cubre todas las áreas de la organización.

El correo, la ofimática y otras herramientas de colaboración que utiliza la empresa son servicios en la nube (CLOUD) con el proveedor Google.

Se utiliza telefonía IP mediante una central Denwa y dos centrales Asterisk que se integran aprovechando las comunicaciones a nivel nacional que mantiene la empresa mediante contrato con la operadora Claro que a través de su infraestructura le brinda el servicio.

Las 5 plantas de producción y los 170 puntos de ventas están conectados al servidor central mediante enlaces punto a punto que les permite realizar en línea todas las operaciones, para ofrecer información en línea y a todos los funcionarios y empleados contar con información actualizada.

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.

2.6 APLICATIVOS DE SISTEMA DE INFORMACIÓN.

La organización cuenta con una robusta aplicación multi-empresa integrada (ERP) llamada SAP la que está compuesta de 13 módulos que soportan las diferentes áreas, la aplicación está desarrollada en lenguaje de programación ABAP y corre sobre ORACLE utilizando el sistema Operativo LINUX Ret Hat, el aplicativo es el número uno a nivel mundial y entre sus fortalezas es porque incorpora las Normas de Seguridad así

como las mejores prácticas para todos los procesos, lleva un control de auditoría que permite garantizar la trazabilidad de todos los procesos, 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

Módulo de Nómina y Recursos Humanos

Parámetros: Control de claves de acceso con parámetros del perfil del sistema

Visualizar parámetros de perfil

Parámetro	Valor parámetro
login/min_password_letters	1
login/password_expiration_time	30
login/min_password_lng	8
login/min_password_digits	1
login/multi_login_users	BASIS,SAP*
login/disable_multi_gui_login	1
login/accept_sso2_ticket	1
login/create_sso2_ticket	2
login/fails_to_user_lock	5
login/fails_to_session_end	3
login/no_automatic_user_sapstar	1
login/failed_user_auto_unlock	0

Figura 2.10 Parámetros de perfil del sistema SAP

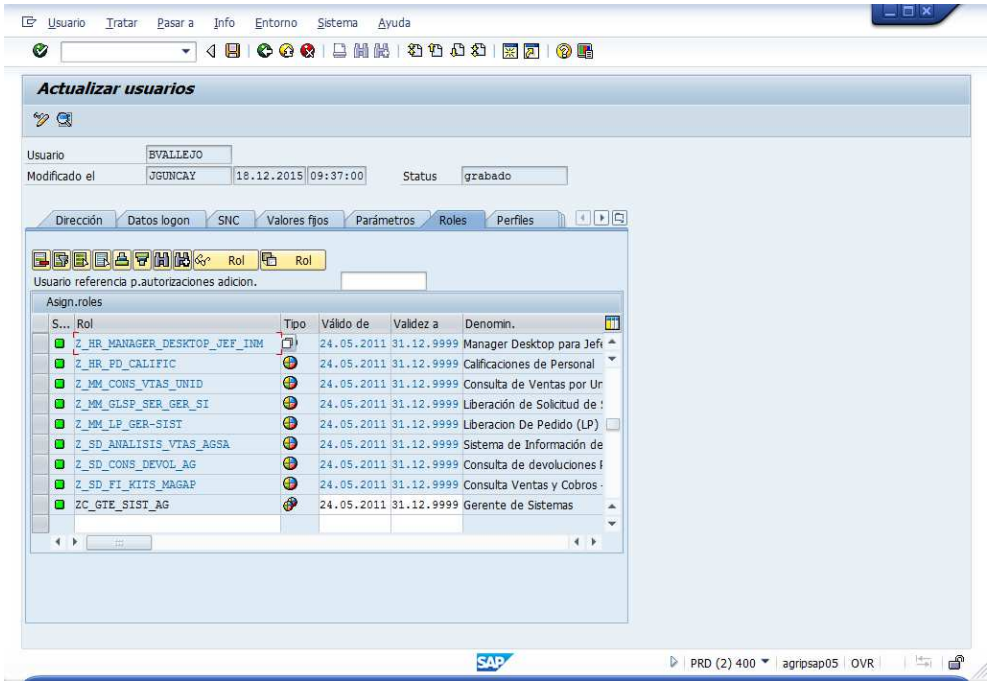


Figura 2.11 SAP: Asignación de roles a usuario

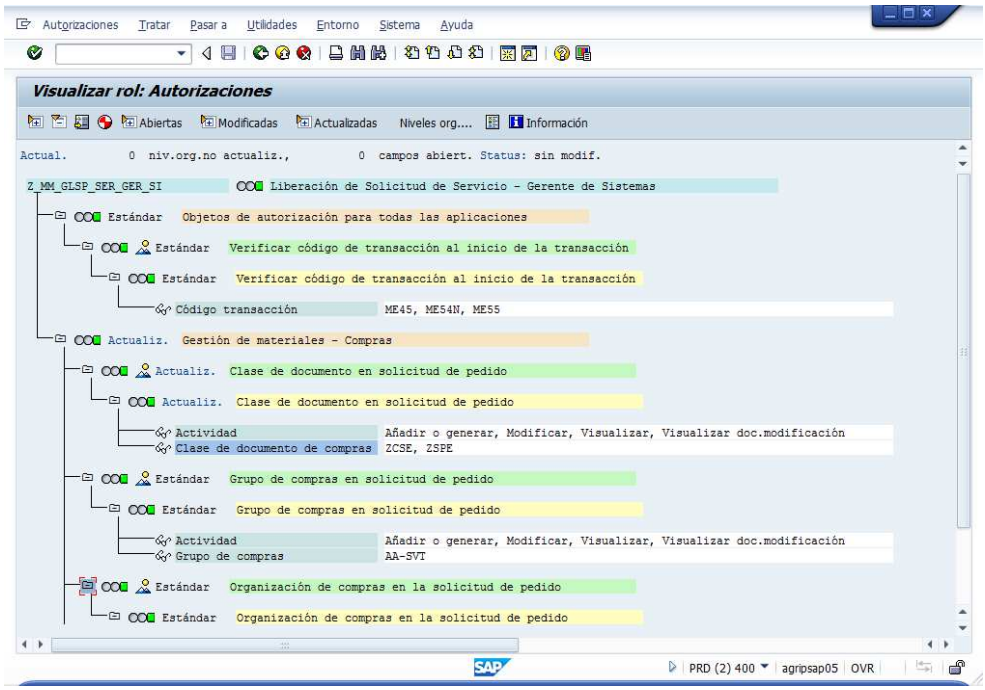


Figura 2.12 Autorizaciones en SAP

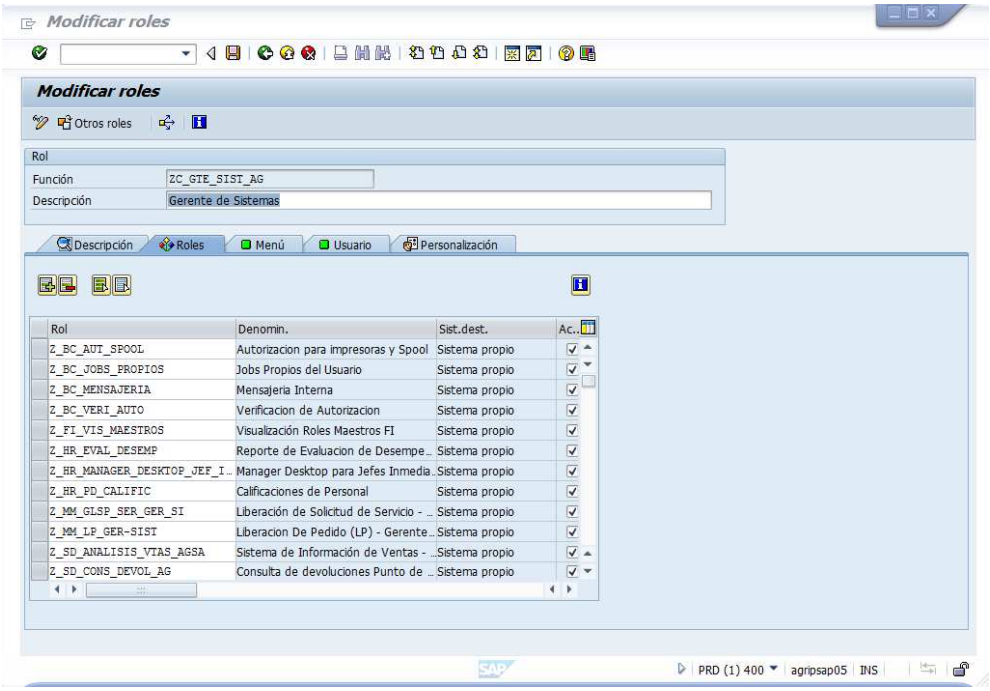


Figura 2.13 Modificación de roles en SAP

Mantiene otras soluciones o módulos para ciertos procesos específicos como son:

Módulo de Control de Facturación Electrónica Agripac-SRI

Portal para consultas de clientes de Facturación Electrónica

Módulo de control de marcaciones de asistencia del personal.

Módulo para control de dispositivos GPS control Sigatoka (banano).

2.7 INSTALACIONES FÍSICAS “CENTRO ALTERNO”

Agripac S.A. cuenta con las instalaciones para un Centro Alterno el mismo que desde hace dos años no está operativo, se encuentra ubicado en el Km. 6.5 de Guayaquil en las instalaciones de la empresa Balanfarina que pertenece al grupo corporativo, el cual incluye las siguientes características:

Dicho centro alterno funcionó durante 10 años como una réplica en línea del servidor de producción, dejó de funcionar hace dos años porque la capacidad de ese servidor es insuficiente para soportar el volumen de transacciones de SAP.

El edificio alterno brinda ciertas condiciones ambientales necesarias para la operación de un Centro Alterno para Recuperación de Desastre que le permita a la empresa poder reactivar las operaciones críticas del negocio, después de ocurrido un desastre mayor que impida el funcionamiento del centro de datos de la oficina matriz.

Dicho centro de cómputo alterno requiere de ciertas adecuaciones físicas que le permita ser funcional como Centro Alterno para un Plan de Recuperación de Desastre y además instalar la infraestructura de TI necesaria para poder operar como centro alterno.

CAPÍTULO 3

SITUACIÓN ACTUAL Y LEVANTAMIENTO DE NECESIDADES

3.1 INTRODUCCIÓN

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 cinco divisiones:

- ❖ División desarrollo de Sistemas.
- ❖ División de Calidad.

- ❖ División de producción
- ❖ División de Seguridad
- ❖ División de Redes

La principal función del departamento de Sistemas de Agripac S.A. es proveer de información oportuna, efectiva y confiable a todas las áreas de la organización, definir los objetivos estratégicos de TI para los siguientes cinco años, los mismos que deben estar alineados con los objetivos estratégicos de la organización, proveer y administrar de manera eficiente los recursos tecnológicos de TI a los usuarios de la organización.

Para una mejor administración y control de TI, el departamento de sistemas mantiene una política de seguridad, actualmente posee Políticas y Procedimientos para cada uno de los procesos y demás servicios que brinda a todas las áreas de la organización, el cumplimiento de lo establecido en las políticas y procedimientos son cuidadosamente auditados cada año por las auditorías externas.

3.2 LEVANTAMIENTO DE REQUERIMIENTOS

La empresa tiene automatizado e integrado todos los procesos del negocio y requiere estar preparada para poder reiniciar sus operaciones

inmediatamente después de ocurrido un evento mayor considerado como desastre que destruya de manera total o parcial el centro de cómputo de la oficina matriz, de esa forma salvaguardar la existencia y la imagen de la empresa.

Considerando que el Plan de Recuperación de Desastre Tecnológico no puede abarcar todos los procesos del negocio, se trabajó con los usuarios claves de cada departamento para identificar aquellos procesos y servicios más importantes y ente ellos se identificó los servicios críticos que permitirán reactivar las operaciones del negocio ante la materialización de un riesgo considerado como desastre, entre los servicios críticos se establecieron los siguientes:

- Proceso de Facturación
- Proceso de Producción
- Proceso de Logística
- Proceso de Cuentas por Cobrar
- Proceso de Cuentas por Pagar
- Proceso de Caja y Bancos

En el análisis de riesgos se deberá determinar la probabilidad de que ocurran dichos riesgos así como el impacto que ocasionarían a las

operaciones del negocio en caso de interrupción de dichos procesos, luego se deberá determinar el tiempo que la empresa podría subsistir sin que dichos procesos estén operativos.

3.3 INFORMACIÓN DEL AMBIENTE DE SISTEMAS

El departamento de Sistemas y Comunicaciones TI define los objetivos de tecnología y comunicaciones de la empresa, brinda información a las diferentes áreas de la organización, es responsable de las decisiones de compras de hardware y software para apoyar las operaciones del negocio, optimizar de manera eficiente la asignación y uso de los recursos tecnológicos y de garantizar la disponibilidad, confidencialidad y seguridad de la información de la empresa.

El equipo de sistemas y Comunicaciones de Agripac S. A. está conformado por 18 profesionales con mucha capacidad y experiencia, están organizados en varios grupos de especialistas que se encargan de atender y operar todos los servicios que este departamento brinda a las diferentes áreas de la organización.

Las divisiones del departamento de Sistemas y Comunicaciones de Agripac S.A. son las siguientes:

Tabla 3 División del Departamento de Sistemas

División	N. Personas	Ubicación	Especialidad
División Desarrollo	4	Matriz	Programadores
División de Producción	3	Matriz	Consultores Funcionales
División de Seguridad y Basic SAP	3	Matriz	Seguridad
División Redes y Soporte	4	Matriz Plantas	Soporte Hardware soporte software
Help Desk	2	Matriz Quito	Soporte usuarios SAP

Sistemas y Comunicaciones TI está ubicado en el tercero y cuarto pisos de uno de los edificios de la matriz el acceso a dicho departamento es controlado mediante tarjetas de aproximación.

3.4 ADMINISTRACIÓN Y CONTROL DE TECNOLOGÍA DE INFORMACIÓN

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, mapas de infraestructura y 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
- Mapas de Infraestructura, Redes, Enlaces.

El departamento de sistemas es el encargado de brindar el servicio a todas las áreas del negocio, el equipo de sistemas está conformado por 18 personas:

1 Gerente de Sistemas y comunicaciones TI.

1 Sub gerente de Sistemas y comunicaciones TI.

2 Consultores Funcionales

1 BASIS

1 Administrador de la Red

1 Administrador de Seguridad

3 Analistas Programadores ABAP

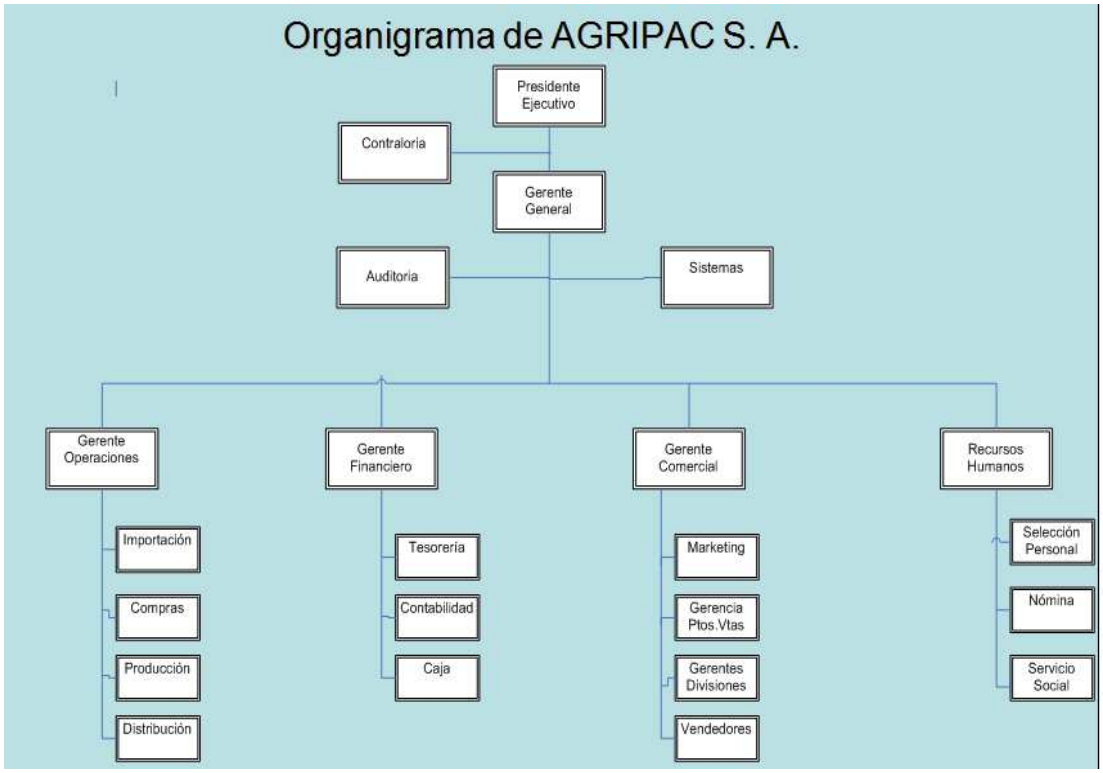
2 Programadores JAVA PHP

3 Técnicos soporte a usuarios

2 Mesa de ayuda.

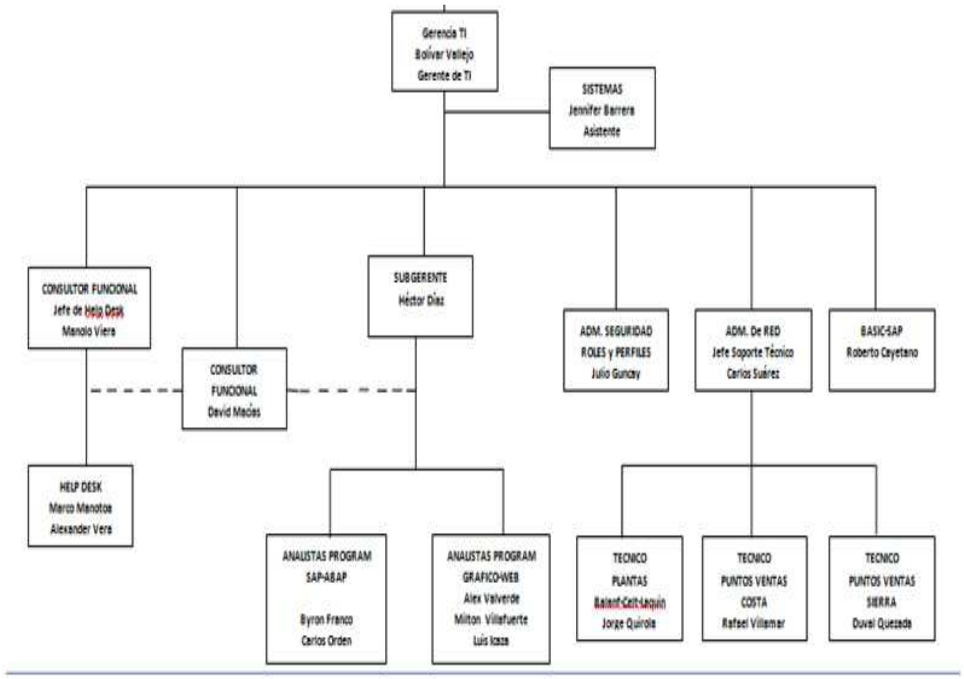
1 Asistente de gerencia

3.5 ORGANIGRAMAS DE LA EMPRESA Y DE TI



16 Figura 3.1 Organigrama de Agripac S.A.

Organigrama de Sistemas y comunicaciones TI



17 Figura 3.2 Organigrama de Departamento TI

3.6 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.

- **Sub Gerente de Sistemas.-** Dirigir, desarrollar y controlar que los proyectos definidos se realicen dentro de los plazos establecidos en el cronograma de trabajo. Mantener la custodia de los códigos fuentes, 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. (BASIS-SAP) -** Controlar que todas las aplicaciones estén acordes con la arquitectura de datos de la entidad y además controla que todos los procesos programados se ejecuten con normalidad.

Control de calidad y paso del área de desarrollo al área de producción**.**

- **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.

❖ **Administrador de Seguridad.-** Garantizar la seguridad, integridad, confidencialidad y disponibilidad de los servicios de acceso a la red de la organización. Coordinar con el Gerente de Sistemas los requerimientos y políticas, que garanticen el acceso de los usuarios internos y externos a la red.

❖ **Consultores Funcionales.-** Coordinar con la Subgerencia 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-Soporte 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.

❖ **Mesa de Ayuda (Help Desk).-** Apoyo a los usuarios finales con en la solución de problemas o requerimientos, especialmente a los puntos de ventas que se encuentran a lo largo de todo el país, realizar las pruebas de las modificaciones y nuevos requerimientos.

❖ **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.

3.7 INFRAESTRUCTURA TÉCNICA

La infraestructura técnica del departamento de Sistemas y Comunicaciones TI de Agripac S. A. es muy robusta y soporta todos los requerimientos de información y demás servicios que brinda este departamento a todas las áreas de la organización, cuenta con servidores de arquitectura x86 tecnología BLADE-HP que soportan las diferentes aplicativos, varios servidores x86 y appliances, también cuenta con dispositivos de almacenamiento Storages de alta disponibilidad de 30 TB con discos SSD, la seguridad de la información así como el control de acceso, spam y virus es protegida por Firewall, Proxy y otros dispositivos de reconocida marcas, todos los puntos de ventas remotos están conectados en línea mediante enlaces punto a punto a través de la infraestructura de la operadora celular Claro, aprovechando la estructura de comunicaciones cuenta también con una red de telefonía IP para la comunicación interna y externa de toda la organización, en todos los puntos de ventas y plantas hay instaladas cámaras de vídeos que permiten mantener un control y monitoreo de dichas localidades.

Actualmente la red de AGRIPAC concentra todos sus servicios en el Data Center de Matriz la conexión a las sucursales es mediante CLARO y 13 Agencias con CNT la navegación de internet es balanceada por el UTM con salida a internet filtrada en permisos, políticas y calidad de servicio (QoS).

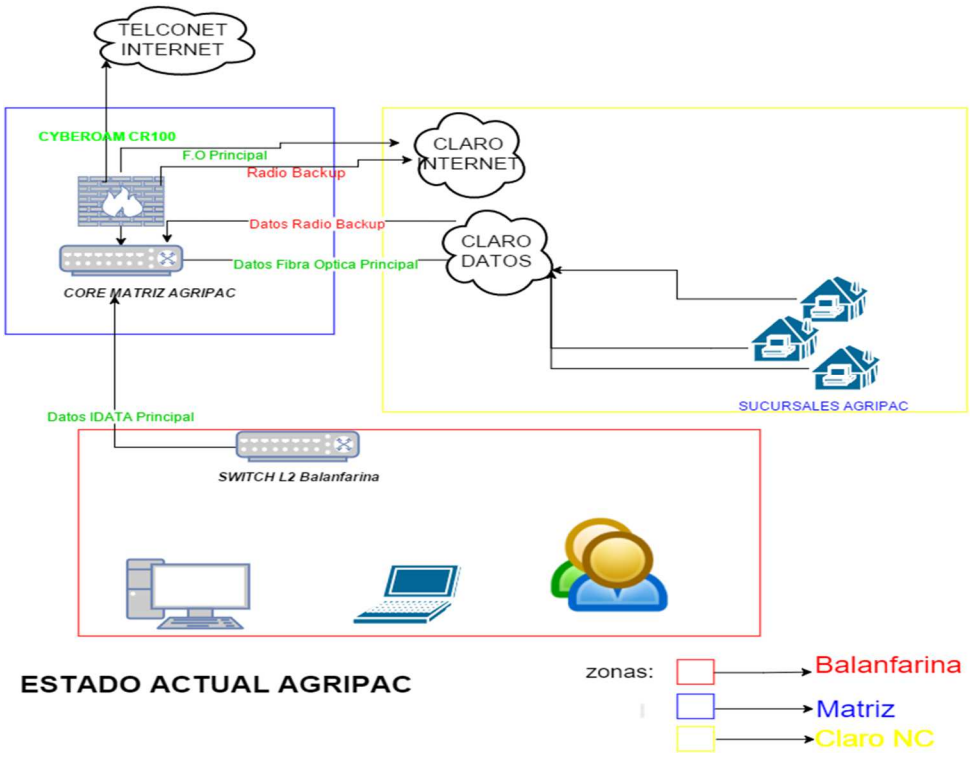


Figura 3.3 Estado Actual de la WAN de Agripac

HARDWARE

HP BLADESYSTEM ONBOARD

Tabla 4 HP BladeSystem Onboard

PARTE	MODELO	NUMERO
Chasis –HP	Enclosure	Hp700
System	BladeSystem	c7000 Enclosure G2
MANUFACTURER	HP	
SERIAL NUMBER		USE0160NRM
PART NUMBER		507019-B21

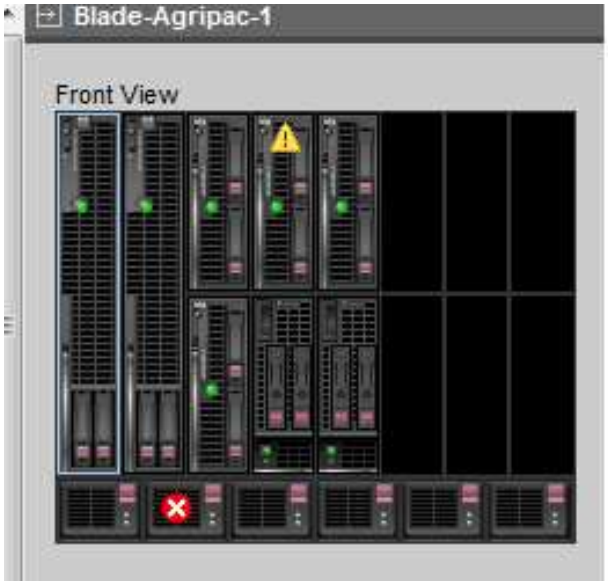


Figura 3.4 Vista Frontal de HP BladeSystem, 16 servidores

Figura 3.5 Vista posterior de HP BladeSystem Fuentes redundantes

Tabla 5 Storage o unidades de almacenamiento de información

Storage	Sistema Operativo	Base de Datos	Capacidad	Discos SSD	Discos SAS 15K
Hitachi HUS 110	Linux Ret Hat	Oracle	39 TB	27 x 200GB	56 x 600GB
Hitachi AMS 2100	Linux Ret Hat	Oracle	19.8 TB		44 x 450 GB

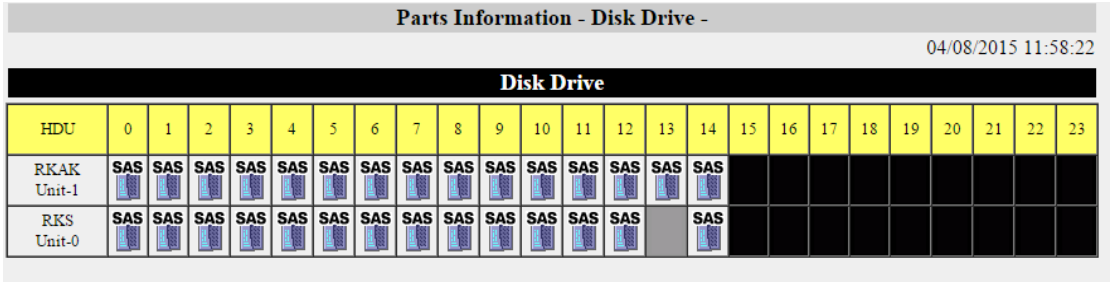


Figura 3.6 Información de los Discos de Calidad y Desarrollo

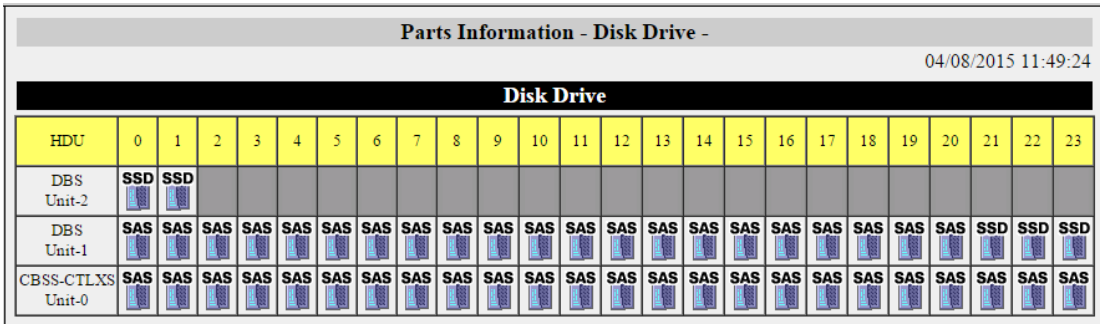


Figura 3.7 Información de los Discos de Producción

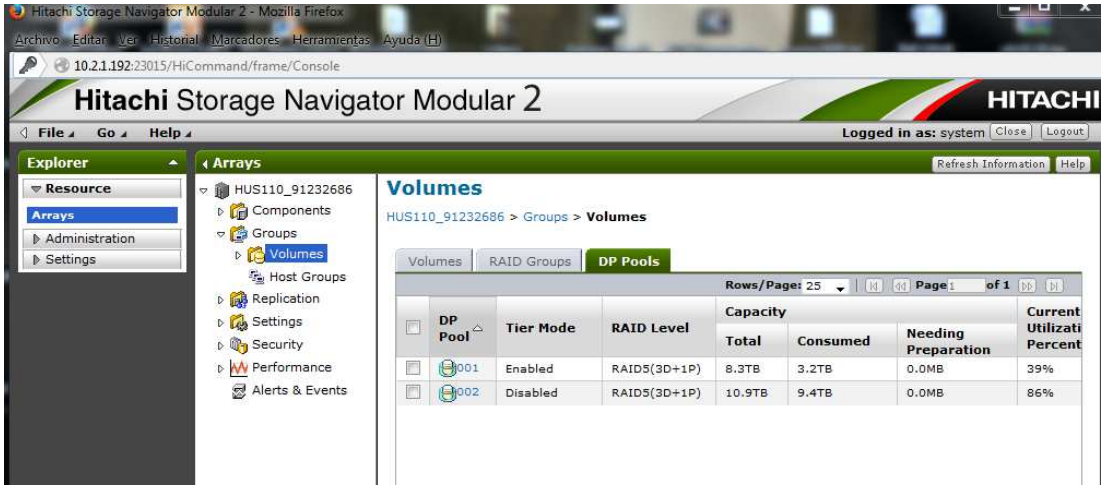


Figura 3.8 Administración Web del Hitachi Storage

Tabla 6 Licencias

Aplicativos	Módulos	Licencias
SAP R3	13	700
Facturación Electrónica	1	1000
Nóminas HCM	3	1500
Módulo Control Personal	3	1500
Control Sigatoka GPS	2	200
Control de Cámaras	1	100
Control de Básculas	1	50
Digitalización Documentos	2	100

Infraestructura de Comunicaciones

Las agencias de Agripac distribuidas en todo el país en su mayoría están interconectadas a la oficina Matriz mediante la red de DATOS de CLARO, también existen ciertas agencias que usan la red de datos de CNT, uno de los puntos de concentración importantes es la RBS NUEVO CARMEN, en esta RADIOBASE se tiene 2 enlaces uno por fibra óptica que actúa como principal y un enlace de respaldo vía radioenlace.

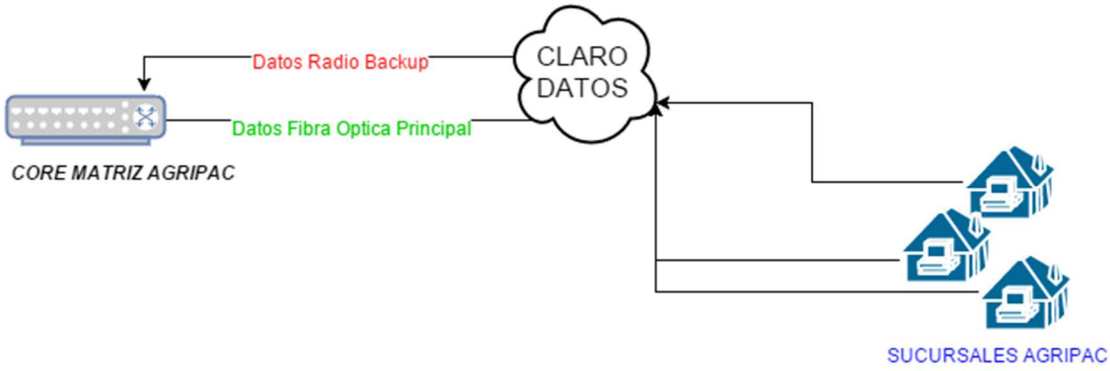


Figura 3.9 Esquema de Conexión entre la Matriz y las sucursales

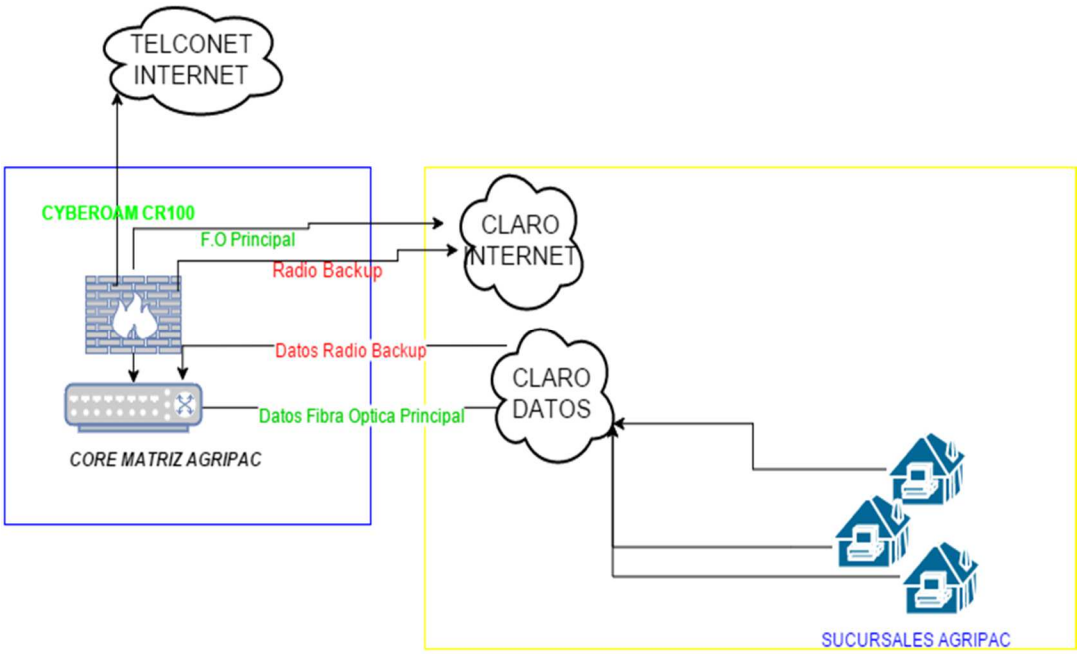
INTERNET:

Agripac Matriz cuenta con servicio de Internet mediante 2 Enlaces de 20 Mbps con ISP diferentes lo que le permite contar con un backup de contingencia en este importante servicio.

- 20 Mbps con CLARO

- 20 Mbps con TELCONET

Estos enlaces recaen en el UTM de seguridad perimetral CYBEROAM CR100 el cual además de las características de firewall de generación avanzada permite hacer el balanceo de la carga de internet con los 2 proveedores.



25 **Figura 3.10 Enlaces WAN de Agripac**

3.8 APLICACIONES

La organización cuenta con una robusta aplicación multi-empresa integrada (ERP) llamada SAP/R3 la que está compuesta de 13 módulos que soportan las diferentes áreas, la aplicación está desarrollada en lenguaje de programación ABAP y corre sobre ORACLE utilizando el sistema Operativo LINUX Ret Hat, el aplicativo es el número uno a nivel mundial y es muy reconocido especialmente en los países desarrollados porque lo utilizan las grandes Corporaciones a nivel mundial, el soporte y mantenimiento está a cargo del equipo del equipo de sistemas de la empresa lo que le permite reaccionar de manera ágil ante cualquier emergencia, además se mantiene un contrato de soporte con el proveedor quien tiene asignado un canal local que se encarga de atender o escalar cualquier problema mayor que requiera asistencia del fabricante, 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

Módulo de Nómina y Recursos Humanos

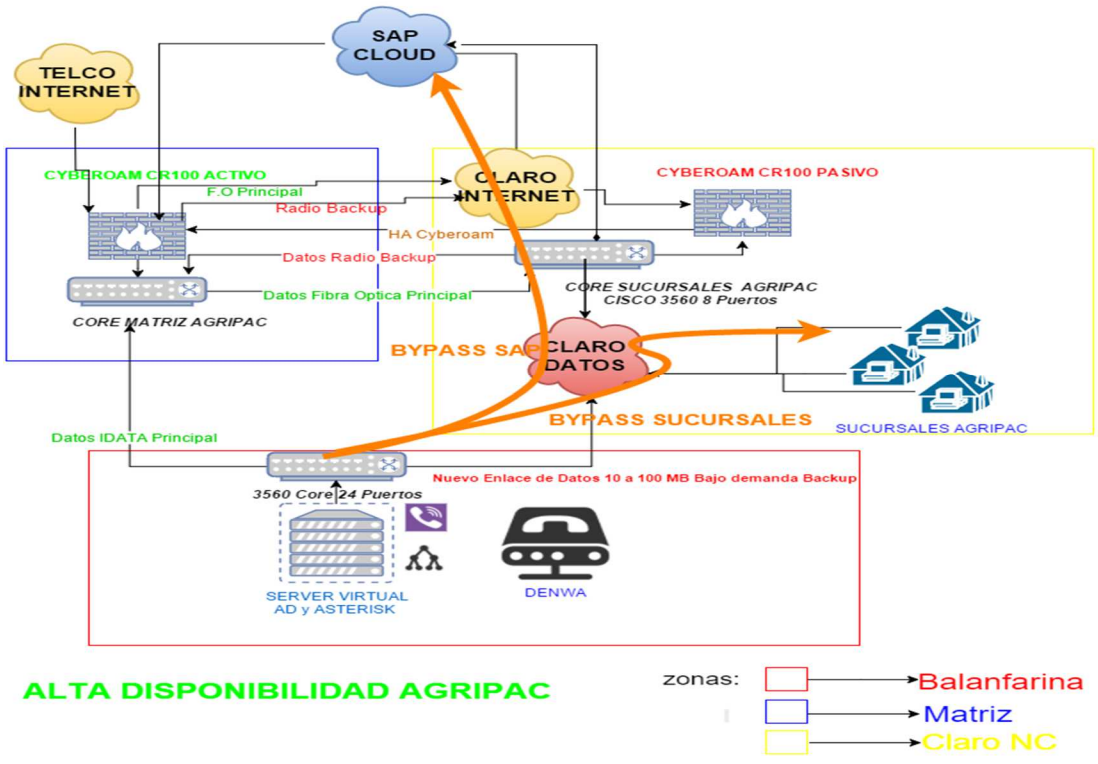
CAPÍTULO 4

ANÁLISIS Y DISEÑO DEL PLAN DE CONTINUIDAD DE NEGOCIO Y DE RECUPERACIÓN DE DESASTRE

4.1 ALCANCE DEL PLAN DE CONTINUIDAD DE NEGOCIO Y RECUPERACIÓN DE DESASTRE.

Este Plan de Continuidad de Negocio y Recuperación de Desastre [11] incluye establecer en la nube (cloud) un backup en línea del servidor de producción y análisis de datos, así como la activación de un Centro Alterno en las instalaciones de la Planta “Balanfarina” ubicada en el Km 6 en la vía Durán Tambo, que permita la recuperación de los procesos críticos del negocio antes del Máximo Periodo Tolerable de Interrupción (MPTI).

En este proyecto se encontrarán procedimientos propios de un Plan de Emergencia para la recuperación y operación de los procesos críticos de AGRIPAC S.A. Por lo tanto, este documento no incluye los procedimientos para la respuesta a incidentes ya que la empresa AGRIPAC S. A. 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 y evacuación.



26 **Figura 4.1 Alta Disponibilidad**

Explicación de la solución:

Se distribuye importancia de cada ubicación por zonas tal como lo describe la imagen Matriz, Balanfarina y el punto de conexión (CLARO NUEVO CARMEN).

Los cambios a realizar son ubicar un SWITCH de capa 3 en la Radio base de Nuevo Carmen y concentrar el enrutamiento en la Radio Base los beneficios de hacer esto son los siguientes:

- ✓ Energía eléctrica ininterrumpida con UPS y Generador
- ✓ Aires acondicionados de precisión
- ✓ Conexión local datos e internet CLARO (Puerto Ethernet)

De esta manera se convierte a nivel de enrutamiento a Matriz y a Balanfarina se convierten circuitos de Agencias Principales. En el caso de una caída hacia las 2 redes de servidores en matriz 10.2.1.0 y 10.1.1.0 el protocolo de enrutamiento redirigirá automáticamente este tráfico al data center de Backup en Balanfarina.

PROTOCOLO ENRUTAMIENTO.-

El tipo de enrutamiento que se utilizara será el OSPF creado también en zonas (Backbone, Matriz, Balanfarina) con el uso de este protocolo se obtienen los siguientes beneficios:

✓ Debido a las bases de datos de estados de enlaces sincronizadas, los "router" OSPF convergerán mucho más rápido que los "routers" RIP tras cambios de topología. Este efecto se hace más pronunciado al aumentar el tamaño del AS.

✓ Incluye encaminamiento TOS ("Type of Service") diseñado para calcular rutas separadas para cada tipo de servicio. Para cada destino, pueden existir múltiples rutas, cada una para uno o más TOSs.

✓ Utiliza métricas ponderadas para distintas velocidades el enlace. Por ejemplo, un enlace T1 a.544 Mbps podría tener una métrica de 1 y un SLP a 9600 bps una de 10.

✓ Proporciona balanceo de la carga ya que una ruta OSPF puede emplear varios caminos de igual coste mínimo.

✓ OSPF soporta rutas específicas de hosts, redes y subredes.

✓ OSPF permite que las redes y los hosts contiguos se agrupen juntos en áreas dentro de un AS, simplificando la topología y reduciendo la cantidad de información de encaminamiento que se debe intercambiar. La topología de un área es desconocida para el resto de las áreas.

El proceso se realizara de la siguiente manera, el proceso de enrutamiento y conexión principal es el enlace de datos que dirige su tráfico hacia el switch core en la red de Matriz esta vendría a ser la zona principal, La zona

Backbone la delimitaremos a los equipos y redes de CLARO ya que este sería el discriminador del uptime de las zonas (Matriz/Balanfarina), en una zona Backup estaría la red de Balanfarina que al momento de detectar una caída(Parametrizable) en un corto tiempo restructurara su tabla de ruteo haciendo Bypass a Matriz y conectando directamente a Balanfarina con las sucursales.

El restablecimiento de las conexiones aun es dependiente de re apuntar los servicios a las nuevas ubicaciones

Ejemplo:

Tabla 7 Direccionamiento IP para ruteo de enlace a centro alterno

Dirección IP	Servicio
10.2.1.196	SAP
10.1.1.2	Proxy UTM
10.2.1.11	AD
10.2.1.5	ASTERISK-DENWA

Por lo que los servicios virtualizados en modo stand by nos ayudaran a encender estos servicios en los servidores nombrados y lograr el restablecimiento sin cambios en los usuarios.

ENLACE NUEVO BALANFARINA:

Para la aumentar la confiabilidad del enlace de Balanfarina se debe de instalar un circuito de 10 Mbps bajo demanda con la RBS de Nuevo Carmen la cual en un momento de requerido se puede aumentar el ancho de banda de este a 100Mbps.

UTM de alta disponibilidad ACTIVO/PASIVO

El UTM CR100 de backup (Pasivo) se configurara conjuntamente con el SWITCH de capa 3 para realizar los servicios de:

- NAT
- PORT FORWARDING
- WAF (Web Application Firewall)
- PROXY WEB
- PERMISOS

- ZONA DMZ

- AUTENTICACION

Se interconectara el CR100 de Matriz con el CR100 de Nuevo Carmen para tener una copia en caliente de las configuraciones y servicios provistos por el UTM es decir en el caso de la pérdida del UTM principal automáticamente el UTM Pasivo entra en funcionamiento manteniendo los servicios de Navegación de internet, Correos Gmail, etc.

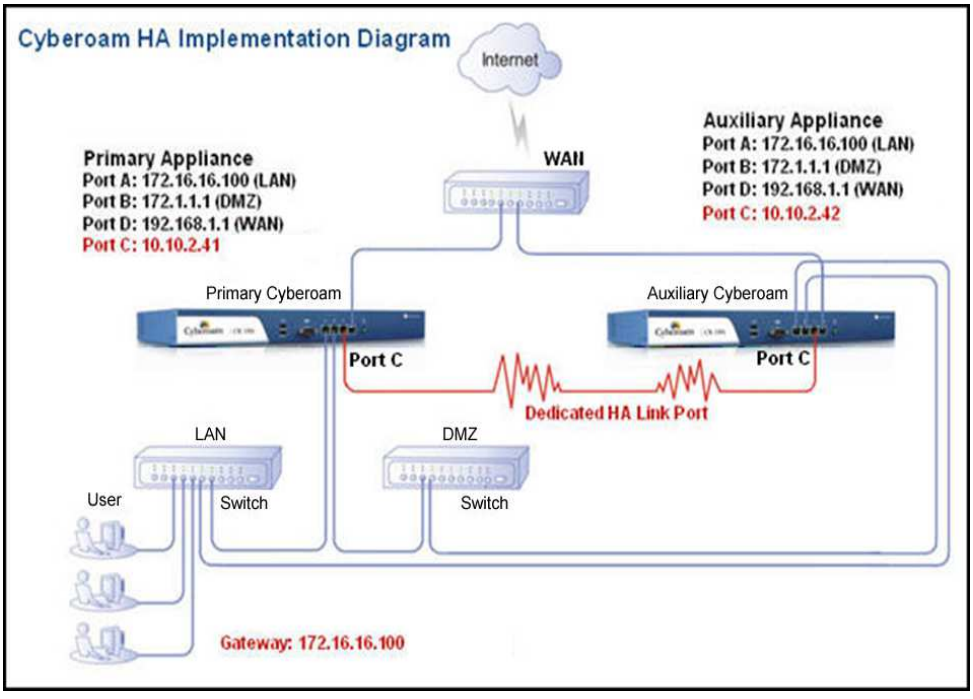


Figura 4.2 Diagrama Cyberoam para enrutar enlaces al centro alterno

SERVIDOR VIRTUAL:

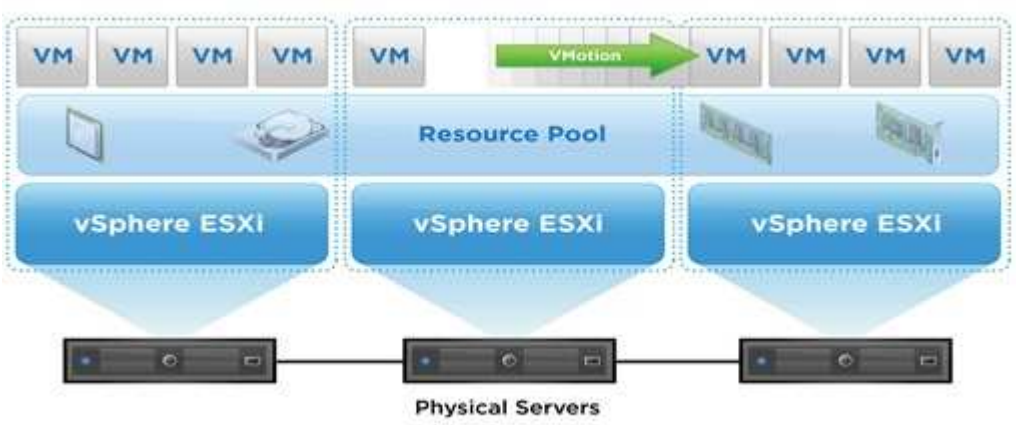


Figura 4.3 Virtual Server en centro alterno para contingencia

Se deberá ubicar un servidor físico en Balanfarina el cual debe de ser instalado con un sistema operativo de Virtualización y dentro de su Hypervisor se crearan las siguientes Máquinas virtuales:

- Active Directory (3 Copia) 10.2.1.11 y 10.2.1.6
- DNS server
- WEB Services facturación electrónica
- Asterisk

En este servidor se deberá de configurar un Domain Controller de respaldo que contenga la copia activa de los servidores de dominio principales

ubicados en Agripac Matriz estos servidores son el 10.2.1.11 y 10.2.1.6. Este nos servirá para mantener los login y autenticación de los usuarios ante la posible pérdida de los ubicados en Matriz.

En el mismo servidor se deberá instalar un servidor de telefonía Asterisk con la misma versión del que da soporte a las sucursales para realizar un backup offline de las extensiones de telefonía de manera que este entre en funcionamiento al no detectar conexión con Matriz.

El servidor deberá tener las siguientes características:

- ✓ 32 GB RAM
- ✓ Arreglo de Discos RAID 5 Discos SAS
- ✓ 1 o 2 Procesadores
- ✓ 4 NIC GigaEthernet

DENWA BALANFARINA

Adicional a esto se deberá ubicar una central telefónica DENWA (Appliance) que tenga las configuraciones para las extensiones que actualmente utiliza las oficinas de Matriz.

SWITCH CORE BALANFARINA

En Agripac Balanfarina se deberá de instalar un SWITCH DE CORE que soporte la cantidad de MPPS procesamiento y throughput que se requeriría al momento de transformarse en el Data Center Activo este deberá estar previamente configurado de tal manera que no requiera intervención el usuario y brinde la confiablidad necesaria al tráfico de datos de los servicios de la red.

SAP Y REPLICACION

Para el sistema ERP SAP al estar alojado en la Nube [7] aseguramos su acceso mediante el servicio a internet y las políticas y configuraciones necesarias en el UTM:

Para la Nube del SAP existen 2 tipos:

- NUBE Publica (Publicada al Internet)
- NUBE Privada (Interconexión con la red de datos de Agripac)

REPLICA NUBE PRIVADA

En el caso de una nube privada la interconexión se debería realizar uniendo a L3 y Claro con un Crossconnect en Nuevo Carmen de esa forma

Matriz no se convertiría en un único punto de fallo sino que tendríamos la alternativa de Balanfarina para la réplica de datos.

REPLICA NUBE PÚBLICA

Si la nube es publica el servicio de internet con el UTM en HA ubicado en la RBS de Claro nos asegura su acceso y replicación.

Para el acceso ininterrumpido de las conexiones a SAP existen 2 opciones:

1) Que la conexión a SAP sea realizada mediante Agripac Matriz, si es de esta manera la Nube del SAP será accesible mediante el switch de CORE de Matriz interconectado a la RBS de Claro en Nuevo Carmen.

2) Que la conexión a SAP sea mediante el Switch de Core Ubicado en Claro en Nuevo Carmen de esta manera el Switch de Core ahí instalado mediante el OSPF realizaría un Bypass entre las sucursales y Balanfarina para dar acceso a SAP ya sea mediante enlace de Datos o Internet.

EQUIPOS Y ENLACES REQUERIDOS:

Para la implementación del DRP [8] se necesitan lo siguiente:

Entre los principales puntos que deberán considerarse son los siguientes:

1. El backup en la nube (cloud) deberá estar en un data center preferentemente ubicado fuera del país, (recomendado Bogotá), el proveedor deberá cumplir con todas las exigencias que se requiere para ofrecer este tipo de servicio el mismo que deberá ser certificado con la Normativa TIER IV, que garantiza la disponibilidad del servicio y contar con el soporte técnico certificado para SAP (24 x 7) además de tener redundancia para la parte eléctrica, UPS, climatización, etc.

2. Se requerirán 8 horas a partir de la declaración de la contingencia para habilitar el Plan de Recuperación de Desastre, en ese tiempo deberán ejecutarse de manera coordinada todas las actividades contempladas en el Plan de Continuidad de Negocio, los tiempos son los siguientes:

Tabla 8 Tiempos para cambiar de status de Réplica a Productivo

N.	Actividad	Tiempo en Horas
1	Comunicar a proveedor de la nube para cambiar el status del servidor de réplica a productivo y levantar el motor de SAP en la nube.	2 Horas
2	Activar el motor de SAP en la nube con todos los servicios y accesos	1 Horas

2	Coordinar con el proveedor de comunicaciones de las plantas y puntos de ventas para cambiar el ruteo de los enlaces para que apunten al servidor de la nube.	2 Hora
3	Coordinar con los proveedores de Internet para que los enlaces de la matriz sean ruteados al centro alterno	1 Hora
4	Habilitar la red y servidor de autenticación y accesos del centro alterno	1 Hora
5	Activar Claves de accesos a usuarios de procesos críticos desde Centro Alterno	1 Hora

3. El Centro Alterno de Operaciones de AGRIPAC S.A. estará ubicado en el segundo piso de las instalaciones de Balanfarina ubicada en el Km. 6 ½ de la vía Duran-Tambo.

4. Se debe dotar de computadoras personales (Laptops) al personal de responsable de procesos críticos, quienes deberán tenerlas siempre disponible para ser utilizadas en caso de una contingencia.

5. En cada piso se cuenta con los puntos de red necesarios para que el personal de los procesos críticos se pueda conectar en caso de emergencia.

6. El Centro de Operaciones para el personal que maneja los procesos críticos estará ubicado en el segundo y tercer piso de la las instalaciones de Balanfarina.

7. 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.

IDENTIFICACION DE SERVICIOS SENSIBLES:

En conjunto con las diferentes áreas de negocios de la empresa se analizaron los procesos críticos que soportan las operaciones del negocio y se identificaron los procesos que son imprescindibles para la continuidad del modelo de negocios, entre estos los más importantes son:

- ✓ SAP
- ✓ CORREO ELECTRONICO
- ✓ TELEFONIA IP
- ✓ INTERNET
- ✓ AD(Active Directory)

SAP.-

El ERP SAP es la parte medular de la empresa ya que todos los procesos de la empresa están registrados en este sistema de planificación de recursos empresariales. Este sistema tendrá una copia y replica de datos alojada en una nube.

CORREO ELECTRONICO.-

Este servicio esta mitigado porque actualmente está alojado en la NUBE de Google su continuidad depende de que los usuarios tengan acceso a internet en los puertos http, https, y 8080.

TELEFONIA IP.-

El sistema de telefonía para la comunicación entre las sucursales, plantas y oficinas el cual usa el circuito de datos de cada sucursal y un servidor centralizado en los puertos UDP 5060 Y RDP 10000 a 20000.

INTERNET.-

El servicio de internet que principalmente da soporte a Transacciones Bancarias, Facturación Electrónica, Paginas del Gobierno, Venta de Kits de semillas, compras y ventas electrónicas, etc.

ACTIVE DIRECTORY.-

El servicio de controlador de dominio de Windows es una parte importante ya que cuenta con una base de datos de los usuarios, permisos y objetos pertenecientes al dominio de la red de Agripac.

Módulos críticos de SAP

Entre los módulos críticos del aplicativo SAP podemos determinar los siguientes:

- Módulo de Facturación
- Módulo de Finanzas
- Módulo de Producción
- Módulo de Inventario

Escenarios para el Plan de Contingencia.

Para efecto de este Plan de Continuidad de Negocio y de Recuperación de Desastre en conjunto con las áreas del negocio fueron identificados tres escenarios, 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 así como el impacto y los efectos directos y posteriores que ocasionaría en las operaciones del negocio.

Tabla 9 Tipos de Escenarios para Contingencia

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

Para efecto del Plan de Contingencia se consideró la escenario número uno cuya estrategia y acciones a ejecutarse para mitigarlo se detallan en las otras secciones de este capítulo.

Escenario N. 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, incendios, tormentas eléctricas severas, etc.

Los **desastres provocados** son eventos generados por seres humanos tales como ataques terroristas.

Escenario N. 2

Daños en los sistemas de información

Concepto: Existen servicios que no son catalogados como desastres, pero aun 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 N. 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).

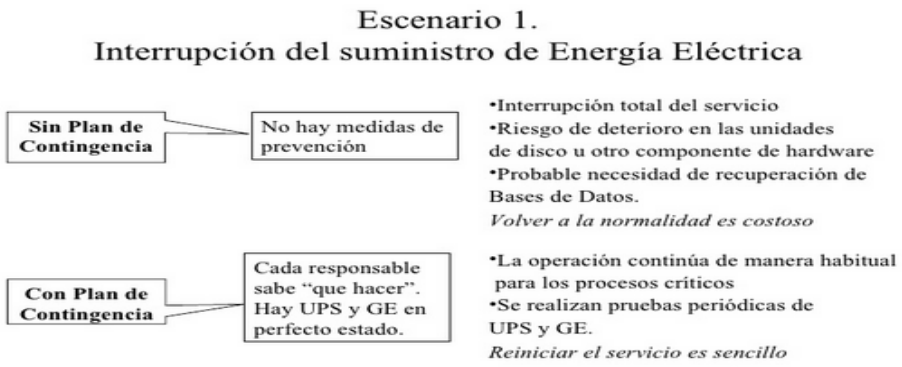


Figura 4.4 Escenario 1 Interrupción Energía

Para la realización de este Plan de Continuidad de Negocio y Recuperación de Desastre solo se tomará en cuenta en Escenario N. 1, es importante dejar establecido que para cada tipo de escenario se deberán definir estrategias orientadas a ese escenario.

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 días o semanas después de materializado el riesgo (desastre). 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.

Las acciones a tomarse para este escenario son las siguientes:

Tabla 10 Acciones a tomarse en Escenario No. 1

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	Equipo de Comunicaciones, Comité de Crisis

(equipos de seguridad) nombrados para estos casos (según Plan de Respuesta a Crisis). [Anexo de contactos]	
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, Transmedical). 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 de 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 alterno.	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

Es por ello que el desarrollo de este Plan se enfocará en las actividades del área de sistemas TI, con las acciones que 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, estos 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.

Figura 4.5 Diferentes tipos de desastres

4.2 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 o críticos y los diversos riesgos que les pueden afectar: intencionados, negligencias o eventos naturales. Entre los riesgos más significativos y que afectarían al negocio tenemos:

RIESGOS INTENSIONALES

- Robo de Equipos

- Alteración o daño de información por ataque de Virus / Hackers
- Ataques terroristas / Amotinamiento de civiles

RIESGOS POR NEGLIGENCIA

- Errores Humanos / Falta de capacitación de Personal (interno y externo)
- Mala configuración de equipos de Telecomunicaciones
- Falta de mantenimiento en equipos eléctricos
- 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 [9]

- Incendios
- Terremotos

- Tormentas eléctricas

Al ser una empresa comercial sus procesos más importantes son aquellos orientados a la venta y servicio al cliente, proveedores, sistema financiero y su capital humano, entre los procesos críticos y directamente vinculados al área de sistemas son: Facturación, Abastecimiento, Producción, Inventario, Cobranzas, Cuentas por Pagar y Nómina.

4.3 ANÁLISIS DE RIESGOS DETERMINADOS PARA EL ÁREA DEL NEGOCIO

Una interrupción de los proceso en el área de TI afectaría considerablemente a las operaciones y a la imagen de la empresa, pudiendo ocasionar pérdidas irremediables si la interrupción es por un tiempo superior al tiempo máximo de tolerancia del proceso.

Entre los riesgos más críticos para el área del negocio 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.

Cuadro de Análisis de Riesgos asociados al área del negocio

En los siguientes cuadros podemos apreciar los riesgos asociados al negocio así como la probabilidad que ocurran y en caso de ocurrir cuál sería su impacto y la severidad de dicho impacto, para determinar la escala de mediciones se realizaron encuestas a ejecutivos y usuarios claves de los procesos, pero ello se utilizaron formularios con preguntas cuyas respuestas fueron tabuladas y graficadas en una matriz de calor donde se puede apreciar de manera objetiva los riesgos potenciales que amenazan a la organización, lo que hace indispensable la implementación de este Plan de Continuidad de Negocio y Recuperación de Rescate.

4.4 ANÁLISIS DE RIESGOS DETERMINADOS PARA EL ÁREA DE TI

Para un mejor análisis de riesgos para el área de TI se elaboró una matriz de riesgos en la que se consideraron los principales riesgos a los que se están expuesto.

MATRIZ DE RIESGO DE VULNERALIDADES PARA EL AREA DE TI.

Tabla 11 Matriz de riesgo de vulnerabilidades TI

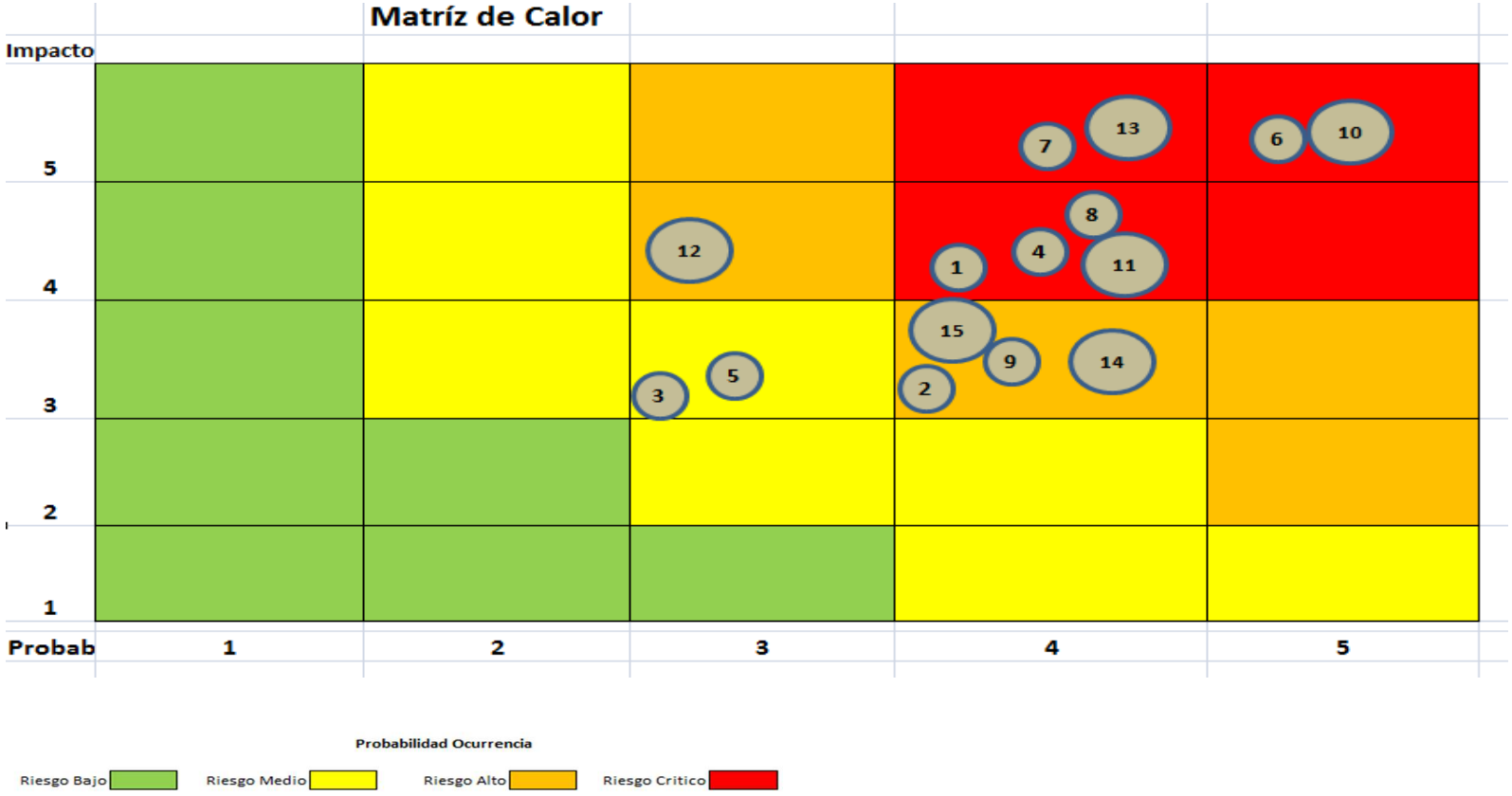
N.	TIPO DE PERDIDA	EVENTO DE RIESGO	CONTROLES ACTUALES	FACTOR DE RIESGO	AFECTACIÓN
1	Disponibilidad del servicio	Fallo en el Funcionamiento de la aplicación SAP	Contrato Mantenimiento con proveedor	- Tecnología	- Paralización general de la operatividad de la empresa
2	Disponibilidad del servicio	Interrupción de las comunicaciones con las Plantas y Puntos de Ventas	Enlaces principales redundantes	- Personas - Tecnología	- Tiempo prolongado sin prestar servicio a los usuarios.
3	Disponibilidad del servicio	Corte de energía prolongado	UPS-Generador eléctrico	- Personas - Tecnología	- Tiempo prolongado sin prestar servicio a los usuarios.
4	Disponibilidad del servicio	Manipulación de la infraestructura de sistemas	Control de acceso físico	- Personas - Tecnología	- Cierre temporal de instalaciones.
5	Disponibilidad del servicio	Suspensión del servicios de proveedor de internet	Enlaces redundante con otro proveedor	- Tecnología	- Tiempo prolongado sin prestar servicio a los usuarios.
6	Disponibilidad del servicio	Incendio en el edificio del Centro de Cómputo	Sistema contra incendio, personal preparado evacuación	- Personas	- Paralización general de la operatividad de la empresa

7	Disponibilidad del servicio	Atentado Terrorista que afecte el centro Cómputo	- Sistema de cámaras de vigilancia.	- Personas	- Paralización general de la operatividad de la empresa
8	Fuga de información	Robo de la información	Control de accesos físico y lógico	Personas tecnología	Pérdidas de activos de la empresa
9	Disponibilidad del servicio	Pérdida de conexión de la red	segmentación de red	- Personas - Tecnología - Procesos	- Tiempo prolongado sin prestar servicio a los usuarios.
10	Integridad de información	Daño o pérdida de información por ataque informático	- Implementación de políticas de navegación y control de acceso a internet.	- Personas - Tecnología	- Tiempo prolongado sin prestar servicio a los usuarios.
11	Integridad de información	Manipulación sensible sin autorización	Control de accesos y perfiles x cargos	Personas tecnología	- Perdida información. - Indisponibilidad de servicios.
12	Integridad de información	Error en programa de aplicativo	Control de modificaciones y pruebas de calidad	- Personas - Procesos	- Insatisfacción en el usuario funcional.
13	Integridad de información	Falla de la base de datos	backup y réplica	- Personas - Procesos	Interrupción de los servicios
14	Pérdida Económica	Pérdida x sustracción de contraseña	Política de caducidad de contraseñas	- Personas - Tecnología	- Registro incorrecto de la información.

15	Imagen Institucional	Vencimiento de licencias de aplicativos	Contrato de licencias vigentes	- Personas	- Multas y sanciones de organismos de control. - Pérdidas económicas para la empresa.

MAPA DE CALOR

Tabla 12 Mapa de calor



La escala y los valores de las mismas fueron determinadas en base a la encueta que se realizó a varios ejecutivos que dirigen los procesos claves.

4.5 ANÁLISIS DE IMPACTO DE NEGOCIO (BIA)

Para efecto del Análisis de Impacto del Negocio (BIA) se trabajó en conjunto con los líderes funcionales de cada departamento se determinaron los procesos más importantes o críticos, habiéndose determinado los siguientes:

Recursos Humanos:

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

Compras/Importaciones

- Proceso de Importación

- Proceso de Recepción
- Proceso de Costos/Liquidación
- Proceso de Proveedores Locales/Exterior
    - Proceso de Cotizaciones
    - Proceso de Órdenes 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 Post-fechados
- Proceso de Tesorería
    - Proceso de Bancos
    - Proceso de Cuentas por Pagar
    - Proceso de Emisión de Cheques
    - Proceso de Pagos Directos / Cobros-Depósitos

- Proceso Contable

Comercial

- Proceso de Marketing
  - Proceso de Diseños y Publicidad
  - Proceso de Promociones
- Ventas
  - Proceso de Facturación
- Proceso Técnico
  - Proceso de Ensayos de nuevos productos
  - Proceso de Control y Trámite de Registros
  - Proceso de Días de Campo
- Puntos de Ventas

Operaciones

- Planificación de distribución y logística
- Proceso de Producción
  - Proceso de Requerimiento/Recepción de Materia Prima

  - Proceso de Requerimiento de Producción
  - Proceso de Manejo de Maestros de Producción
  - 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

El mapa de Calor nos muestra que muchos de los riesgos son altos y otros son muy críticos lo que indica que la empresa tiene una alta dependencia de esos procesos que deben ser controlados y minimizados en el menor tiempo posible.

En las entrevistas con los dueños de procesos se pudo determinar que cuentan con procedimientos manuales definidos en los que se indican las acciones a tomar en caso de prescindir de los procesos automatizados

Pero los procesos manuales se los puede aplicar en temporada baja no así en temporada alta donde el volumen de transacciones es muy alto lo cual sería imposible manejarlos de forma manual.

Analizando la matriz de riesgo se puede determinar que la empresa podría mantener sus operaciones con los procesos manuales por 3 días en temporada baja y un día en temporada alta, el no contar con los procesos automatizados fuera de esos tiempos le ocasionaría un impacto muy alto por el descontrol de la producción, el inventario, la logística, cobranzas, etc., lo que se reflejaría en pérdida de oportunidades de Ventas que conllevan una disminución de mercado y por tanto pérdida de imagen Corporativa.

El alto número de ítems que maneja por líneas de productos en cada una de sus divisiones, 15.000 ítems aproximadamente, hacen muy difícil manejarlos con un proceso manual.

La organización posee una cartera de 95.000 clientes a nivel nacional los mismos que son manejados en línea y de forma integrada en el sistema, ciertos procesos como ingreso de nuevos cliente, autorizaciones, liberación o ampliación de cupos, bloqueo de cuentas, etc., requieren que los oficiales de crédito tengan acceso a dicha información para realizar las gestiones correspondientes, manualmente sería imposible manejar dichos procesos.

Nómina es uno de los procesos que se encuentra apoyado fuertemente con un sistema automatizado y requiere estar respaldado por un backup externo (Cloud) que garantizan su funcionamiento en caso de contingencia.

La empresa requiere de forma urgente contar con una réplica o backup del servidor de producción en la nube (Cloud) más un Centro Alterno para garantizar la operatividad de estos procesos dependientes altamente de tecnología, el tiempo de activación del Centro Alterno debe ser menor que el Máximo Periodo Tolerable de Interrupción (MPTI) de dichos procesos.

4.6 CRITERIOS PARA LA DECLARATORIA DE CONTINGENCIA Y ACTIVACIÓN DEL CENTRO ALTERNO

Los criterios que se han definido para la declaratoria de contingencia y la activación del centro alterno son los siguientes:

Daño parcial o total de la infraestructura de tecnología TI que impida el funcionamiento de los procesos críticos, el daño puede ser por un desastre natural o causado, ejemplo terremoto, incendio o atentado terrorista.

Inconsistencia de la base de datos, aunque sea un daño parcial pero si toma más de tres días para su recuperación deberá activarse el plan de contingencia.

Daño del servidor de producción, aunque se tenga contrato con el proveedor este tipo de daños puede durar varios días lo cual es una causal para la activación del plan de contingencia.

Daño del aplicativo SAP, la instalación y configuración de SAP demanda varios días por lo tanto aunque sea un daño parcial implica la paralización de los procesos críticos por varios días, siendo necesario la activación del plan de contingencia.

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 activar el servidor de backup que se encuentra en la nube (cloud) para ser operado desde el Centro Alterno en modo de emergencia y la declaración de contingencia conlleva a la activación del Plan.

Tabla 13 Criterios Activación del Plan de Contingencia

Criterios	Tipo de Evento	Daño Parcial	Daño Total	Tiempo de Recuperación
Daño Infraestructura TI	Incendio Terremoto o atentado		X	Mayor a 3 días
No funciona Base de Datos	Inconsistencia en datos		X	Mayor 3 días
Daño aplicativo SAP	Fallas en programas	X		Mayor a 3 días
Daño Servidores	Robo, daño o manipulación	X		Mayor a 3 días

CRITERIOS PARA LA ACTIVACION DEL PLAN DE CONTINGENCIA

Los criterios que deben cumplirse para la activación del Plan de Continuidad de Negocio y de Recuperación de Desastre son los siguientes:

- Afectación mayor de las instalaciones de la empresa y de la infraestructura de sistemas causadas por un desastre natural o intencional (atentado terrorista).

- Interrupción de los servicios de sistemas por falla o daño de la base de datos o del aplicativo y que el tiempo de recuperación sea mayor al Máximo Periodo Tolerable de Interrupción (MPTI).

- Para poner a prueba el funcionamiento del Plan de Continuidad de Negocio.

4.7 ESCENARIOS

En base al resultado del *Análisis de Impacto de Negocio (BIA)* y el *Análisis de tiempo de recuperación*, fueron identificados tres escenarios, estos son:

Tabla 14 Escenarios

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

Agripac S.A. debe definir procesos de preparación y prestación de servicios en modalidad de contingencia. Estos tres escenarios están en directa relación con la magnitud de la ocurrencia del evento así como el impacto y los efectos que ocasionaría en las operaciones del negocio.

Escenario N. 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, incendios, tormentas eléctricas severas, etc.

Los **desastres provocados** son eventos generados por seres humanos tales como ataques terroristas.

Escenario N. 2

Daños en los sistemas de información

Concepto: Existen servicios que no son catalogados como desastres, pero aun 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 N. 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).

Para la realización de este Plan de Continuidad de Negocio y Recuperación de Desastre solo se tomará en cuenta en Escenario N. 1, es importante dejar establecido que para cada tipo de escenario se deberán definir estrategias orientadas a ese escenario.

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 días o semanas después de materializado el riesgo (desastre). 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 del área de sistemas TI, con las acciones que 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, estos 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.

4.8 ANÁLISIS DE IMPACTO FINANCIERO

Agripac S. A., depende en un alto grado de los servicios de información y tecnología TI de producirse un desastre natural o provocado que afecte la infraestructura de tecnología que impida mantener operativo los servicios críticos por más de tres días ocasionaría un fuerte impacto financiero a la organización el mismo que se incrementaría significativamente si el tiempo de interrupción de los servicios críticos es superior al Máximo Periodo Tolerable de Interrupción (MPTI), porque no solamente afectaría a los ingresos que deba recibir la empresa por dichos servicios sino que se ocasionaría un descontrol en todas las operaciones de la organización con un impacto financiero muy alto.

Otro análisis financiero desde una óptica simple determina que el impacto financiero que le costaría a la empresa por cada día que no estén operativos los servicios críticos sería un valor muy alto de acuerdo al siguiente análisis.

Tabla 15 Análisis de Impacto Financiero

Análisis de Impacto Financiero

PROCESOS CRÏTICOS	TOTAL MENSUAL	TOTAL POR DIA	TOTAL POR HORA
Ventas Mensual	25.000.000	833.333	104.166
Costos Producción	500.000	16.666	2.083
Sueldos personal *	340.000	11.333	1.416
Recuperación Cartera	23.000.000	766.667	95.833
TOTALES		**1.627.999**	**203.499**

** Personal de Puntos de Ventas, Plantas, cobranzas y Tecnología.

El impacto financiero diario por la interrupción de los servicios críticos es muy alto para la empresa, es mismo que se incrementaría exponencialmente a partir del tercer día, por ello está plenamente justificada la implementación del Plan de Continuidad de Negocio y de Recuperación de Desastre cuya implementación conforme lo plantea este proyecto tiene un costo muy bajo porque aprovechando la evolución de la

tecnología y mejoras de comunicaciones en nuestro país, se escogió la opción de utilizar los servicios de un proveedor de data center para albergar un backup del servidor de producción, lo que implica que la empresa no tenga que realizar una alta inversión para construir un centro alterno de datos, por lo tanto la inversión se limitará solamente a la habilitación de centro alterno para que los usuarios de los procesos críticos puedan operar desde ese sitio ubicado en la planta que tiene Agripac en el Km 6 de la vía Durán Tambo, en el momento que el centro de cómputo actual de la empresa sea inhabilitado por un periodo superior a tres días por la materialización de un riesgo mayor considerado desastre.

El costo para habilitar y dotar el centro alterno de laptops, routers, switch, mobiliario, etc., es mucho menor que invertir en un servidor para mantener una copia o backup del server de producción.

Tabla 16 Costo de Inversión implementación de Centro Alterno

Rubros	Costo	Porcentaje
Hardware nube (cloud)	$ 55.000	44.00 %
Hardware en Centro Alterno	$ 40.000	3.00 %
Enlaces de Comunicaciones	$ 15.000	12.00 %
Mobiliario	$ 15.000	12.00 %
Total	**$ 125.000**	**100.00 %**

Tabla 17 Costo Servicio Cloud y Comunicaciones

	Mensual	Anual
Costo Servicio Cloud y Comunicaciones	**$ 15.000**	**$ 180.000**

La inversión es mínima considerando que se está protegiendo y garantizando todas las operaciones de la organización que vende 300 millones al año, así como la continuidad y existencia misma del negocio en caso de un desastre natural o provocado.

CAPÍTULO 5

IMPLEMENTACIÓN DEL PLAN DE CONTINUIDAD DE NEGOCIO Y DE RECUPERACIÓN DE DESASTRE

5.1 FASES DEL PLAN DE ACCIÓN.

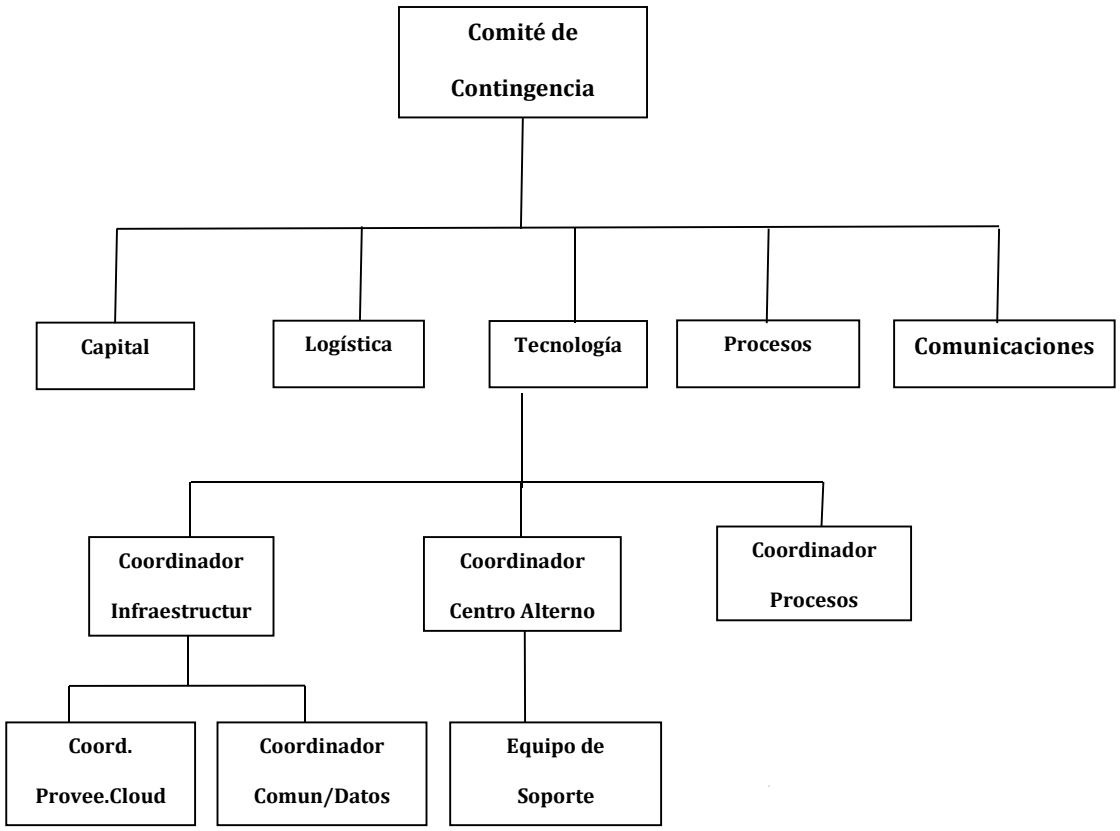
Para la implementación del Plan de Continuidad de Negocio y Recuperación de Desastre es altamente importante que éste sea socializado en todos los niveles de la organización, que exista el compromiso y apoyo de la alta gerencia, que el Comité de Contingencia sea integrado por los usuarios claves de los procesos críticos que forman parte de este Plan, dichos usuarios deberán recibir la información y

capacitación necesaria y el Plan deberá ser probado y actualizado constantemente para garantizar su funcionamiento en el momento que requiera ser activado, para mejor aplicación de este Plan lo hemos dividido en ocho Fases, estas son:

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

5.2 ESTRUCTURA ORGANIZATIVA PARA EL PLAN DE CONTINGENCIA

ORGANIGRAMA DEL COMITÉ DE CONTINGENCIA



5.3 COMITÉ DE CONTINGENCIA

El Comité de Contingencia es el órgano encargado de coordinar, administrar, supervisar, activar y operar el Plan de Continuidad de Negocio y Recuperación de Desastre, está altos funcionarios de la organización así

como por usuarios claves de los procesos críticos que han sido considerados en este plan

Comité de Contingencia

Tabla 18 Comité de Contingencia

#	NOMBRE	CARGO CONTINGENCIA
1	Gustavo Wray	Comité de Contingencia
2	Nicolás Armstrong	Comité de Contingencia
3	Francisco Luna	Comité de Contingencia
4	Almudena Cardenal	Comité de Contingencia
5	Pedro Kan Paw	Comité de Contingencia
6	Wendy Desideiro	Equipo de RR. HH.
7	Lorena Hidalgo	Equipo de RR. HH.
8	Gustavo Wray	Coordinador Comunicaciones internas y externas (Prensa)
9	Rocío Torres	Asistente Coordinador de Comunicaciones
10	Marcia Romero	Equipo de Comunicaciones
11	Francisco Rodríguez	Coordinador de Logística
12	Mauricio Martínez	Asistente Coordinador de Logística
13	Gerónimo Alcívar	Equipo de Procesos
14	Ma. Fernanda Méndez	Equipo de Logística
15	Ma. Dolores Molina	Coordinador de Infraestructura/Evaluación de Daños
16	Haynes Matthew	Asistente Coordinador Infraestructura/Evaluación de Daños

17	Alfredo Noboa	Equipo de Infraestructura/Evaluación de Daños
18	Ec. Manuel Suco	Coordinadora de Procesos
19	Dennys González	Asistente Coordinadora de procesos
20	Laura Delgado	Equipo de Procesos
21	Alexandra Salazar	Equipo de Procesos
22	Bolívar Vallejo	Coordinador de Tecnología
23	Héctor Díaz	Coordinador de Centro Alterno
24	Manolo Viera	Coordinador de aplicativos SAP
25	Roberto Cayetano	Equipo de activación servidor en la nube (cloud)
26	Carlos Suarez	Equipo de comunicaciones y Redes
27	Julio Guncay	Coordinador Seguridad, Roles y Perfiles
28	Jennifer Barrera	Equipo de Soporte a Personal
29	David Macías	Administrador de Ambiente
30	Byron Franco	Coordinador de Ambiente
31	Segundo Méndez	Coordinador de Soporte
32	Alexander Vera	Asistente de Soporte
33	Marco Manotoa	Equipo de Soporte

5.4 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.

5.4.1 EQUIPO: 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 la activación del plan de Contingencia y coordinar la aplicación de los procedimientos para atender la emergencia.

2. Autorizar y coordinar la entrega de los diferentes 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.

5.4.2 EQUIPO: 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.

5.4.3 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.

5.4.4 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.

5.4.5 EQUIPO: DE INFRAESTRUCTURA

Responsabilidades previas a una Contingencia

1. Definir estrategias y coordinar con los proveedores de la nube (cloud) y de comunicaciones para cambiar el status de los servidores de backup a productivo así como los equipos de comunicaciones inmediatamente después que el Comité declare la activación del plan.

2. Organizar y entrenar grupos o brigadas de trabajadores que se encargarán de la activación del centro Alterno.

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.

5.4.6 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.

5.4.7 EQUIPO: 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.

5.4.8 EQUIPO: 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 enrutamiento 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.

5.4.9 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. Respaldar 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.

5.5 ESTRATEGIAS DE RECUPERACIÓN

Una estrategia de recuperación es una combinación de medidas preventivas, detectivas y correctivas, que ayudan a eliminar la amenaza, minimizar la probabilidad de que ocurra y a minimizar o mitigar su 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)*:

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 tomando como base las mejores prácticas recomendadas en la Normativa ISO -22301 en su metodología.

5.6 ALTERNATIVAS DE RECUPERACIÓN

Las interrupciones que impiden el funcionamiento de los centros de cómputo por largo tiempo resultan frecuentemente muy costosas, en especial cuando son causadas por desastres naturales o causados que invalidan el centro físico primario, estas contingencias exigen alternativas de respaldo en una sede remota, entre las alternativas para Agripac se analizaron las siguientes:

Tabla 19 Alternativas de recuperación

Estrategia	Detalle	Requerimientos adicionales
Hot Site-Cloud	Configurados totalmente y listos para operar en pocas horas.	Personal, enlaces de Internet comunicaciones, desviación de enlaces de plantas, puntos de ventas y activación de Centro Alterno

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.

La alternativa que se eligió es la llamada “Hot Sites Cloud” que permitirá en pocas horas tener habilitados los servicios críticos lo que mitigaría el impacto causado por un desastre.

5.7 ESQUEMA DE PRESTACIÓN DE SERVICIOS EN CONTINGENCIA

Considerando lo importante que son la prestación de servicios durante una contingencia, la documentación donde se detallan cada uno de ellos así como el alcance, los teléfonos de los proveedores y coordinadores de cada

equipo, los recursos que se necesitan y su ubicación, las actividades y responsabilidades de los equipos, etc., estarán disponibles en una carpeta en el servidor que está ubicada en el centro alterno, a dicha carpeta podrán ingresar desde cualquier lugar los miembros de los diferentes equipos a quienes se les asignará una clave de acceso.

Para una mejor prestación de los servicios en contingencia se lo ha clasificado en siete tipos de servicios de acuerdo a los procesos críticos que fueron definidos, estos son:

Escenario: Desastres naturales o provocados

Servicio N. 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.

Tabla 20 Servicio de Mantenimiento de hardware

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, cd de diagnóstico	Ficha de solicitud de servicio de sistemas	Rafael Villamar

Servicio N. 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 SAP

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.

Tabla 21 Servicio de desarrollo en SAP

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 interfaces)	N/A	N/A	N/A	N/A
Pruebas ambiente de pruebas	1 Computador	Servidor de pruebas	Procedimiento de ficha técnica de modificaciones	Manolo Viera
Pruebas paso a producción	1 Computador	Servidor de pruebas	Procedimiento de pruebas de requerimientos y modificaciones	M.Viera J.Guncay

Servicio N. 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.

Tabla 22 Servicios de networking

Elemento Servicio	Equipos	Materiales	Documentos	Responsable
Instalaciones de red	-	Ponchadora, conectores, cuchilla, cable UTP Cat 6ª	Ficha de solicitud de servicio de sistemas	Carlos Suárez
Solución de problemas	1 Computador	Teléfono	Ficha de solicitud de servicio de sistemas	Carlos Suárez / R. Cayetano
Monitoreo red centro alterno	1 Computador	Software licenciado	Acceso a carpeta de servicios	R. Villamar
Monitoreo de enlaces	-	Proveedores contacto permanente	-	Carlos Suárez
Manejo de Seguridad de accesos	Servidor centro alterno UTM	Consola	Procedimiento de manejo y control de accesos	Carlos Suárez Julio Guncay
Manejo de parches SAP	N/A	N/A	N/A	N/A
Correo electrónico	Google	Consola	Validación de accesos	Carlos Suárez
Internet	UTM Cyber Roam	Laptops-modem	-	Carlos Suárez /Líder Tecnología

Servicio N. 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 réplica o backup en la nube (cloud), en las base de datos que resida en el servidor de la nube. 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 de SAP

Mediante este proceso, el responsable firmará, registrará y recuperará los medios magnéticos almacenados conforme se requiera para las operaciones 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.

Tabla 23 Servicio de Administración de Base de Datos

Elemento Servicio	**Equipos**	**Materiales**	**Documentos**	**Responsable**
Instalación de / Base de Datos			Procedimientos de configuración e instalación: Linux - SAP	R. Cayetano
Definición y monitores de replicación	1 Computador	Escritorio	Procedimiento de replicación	R. Cayetano
Respaldo base de datos	Storage Hitachi	Discos SAS-15K	Procedimiento respaldo de base de datos Bitácora de respaldos sistema	R. Cayetano
Respaldos sistema operativo	Storage Hitachi	Discos SAS 15k	Procedimiento de respaldo de “file system” del sistema (Linux). Procedimiento de respaldo del sistema operativo (Windows).	R. Cayetano
Respaldo datos usuarios	N/A	N/A	N/A	N/A
Respaldo de programas fuente/objeto	Unidad Tape externa	Disco externos SAS 15k	Llevados a BB	Alterno.
Respaldo de Base de Datos	Unidad Storage Hitachi	N/A	Configuración de instalación, usuarios, aplicaciones y datos	R. Cayetano

Servicio N. 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.

Tabla 24 Servicio de Help Desk

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 acceso Aplicaciones	-	Instaladores.	Procedimiento de configuración e instalación	
Mov. De equipos	-	-	Solo con aprobación de Líder de Proceso de Negocio	

Servicio N. 6

Nombre: Adquisiciones.

Descripción:

Este servicio se encuentra descentralizado a Compras y no se provee 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 buscara en la lista de proveedores definidos para la contingencia, se cotizará y se pasará luego al proceso de Compras.

Servicio N. 7

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.

Tabla 25 Servicio de soporte administrativo

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

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

Tabla 26 Documentación de requerimientos

Requerimiento	Documento
Lista del personal, con prioridades.	Anexo A
Números de teléfono del personal: celular y convencional, direcciones y correos	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. Nube (cloud), Comunicaciones, Backbone	Anexo C

5.8 PLAN DE ACTIVIDADES DURANTE LA CONTINGENCIA

Plan “Primeros Pasos” para activar la Contingencia

Tabla 27 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 se comunica con los proveedores de la nube (cloud) y de comunicaciones, para que el servidor de backup pase a productivo y sean activados los switch para desviar los enlaces de las plantas y puntos de ventas al servidor de la nube, al mismo tiempo el coordinador del equipo del Centro Alterno toma las acciones para habilitar los servicios del mismo y coordina con el proveedor de comunicaciones para que el centro alterno se conecte con el servidor de la nube. Igualmente se comunica con el responsable del Centro Alterno para que sea activado.
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 para activar los enlaces redundantes
8.	Administrador de Red comunica a Líder de Tecnología y al responsable de Administración de Datos del cambio exitoso al enlace de la nube
9.	Administrador de aplicativo, revisa el funcionamiento de los procesos críticos en SAP
10.	Líder de IT solicita al Equipo de Comunicaciones notificar a las plantas y almacenes continúen su labor de forma degradada a los procesos críticos.

Plan de Actividades durante la Contingencia

Tabla 28 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, Transmédical, Clínica Guayaquil). 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 y TI

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 alterno.	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.

5.9 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:

Tabla 29 Actividades luego de la Contingencia

Actividad	Responsable
Evaluar condiciones del centro de cómputo Principal. Inmediatamente después que el siniestro ha concluido, se	Equipo de Infraestructura

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.	
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.	Comité de la Contingencia
Proceso de Compras Poner órdenes de compra para reemplazo de equipos, órdenes de servicio y/o reparación, en la medida de que sea necesario.	Líder de Tecnología
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.	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 continúo del Plan de normalización de los servicios luego de la Contingencia.	Todos

Pasos para la reactivación del servicio desde Centro de Cómputo Principal

Tabla 30 Pasos para reactivación del servicio del Centro de Cómputo principal

Pasos	Actividad
1.	Líder de tecnología con equipo técnico revisan que las instalaciones para el centro de cómputo están listas, (acometidas eléctrica, UPS, climatización, detector humo, control de acceso, etc.
2.	Líder de tecnología coordina con los proveedores de hardware la instalación y configuración de los equipos de infraestructura (servidores, racks, routers, Switch, etc.)
3.	Equipo de tecnología proceden con la configuración de los equipos de infraestructura
4.	Líder de tecnología coordina con proveedor de Data Center la restauración de la base de datos y configuración de SAP en los nuevos servidores de matriz.
5.	Líder de tecnología coordina con proveedor de comunicaciones cambio de ruteo de los enlaces de las plantas y sucursales al centro de datos de la matriz
6.	Administrador de red define y pasa información del servidor del Active Directory del Centro Alterno al Servidor de Matriz
7.	Administrador de red realiza pruebas y certificación de los puntos de red (voz y datos)
8.	Administrador de red y Administrador de Base de Datos realizan pruebas y test de todos los servicios
9.	Líder de tecnología comunica a proveedor de la nube cambiar servidores de producción a réplica y bajar servicios de SAP
10.	Se inicia la prestación de servicios desde centro de cómputo matriz

11.	Líder de tecnología comunica fin de la Contingencia
12.	Líder de tecnología coordina con su equipo el mejoramiento continuo del Plan de Contingencia

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

CAPÍTULO 6

PRUEBAS Y ANÁLISIS DE RESULTADOS

6.1 PRUEBAS DE CONECTIVIDAD CON DATA CENTER (NUBE) DE PROVEEDOR

La conectividad con el proveedor de la nube debe realizarse bajo el siguiente esquema de comunicaciones:

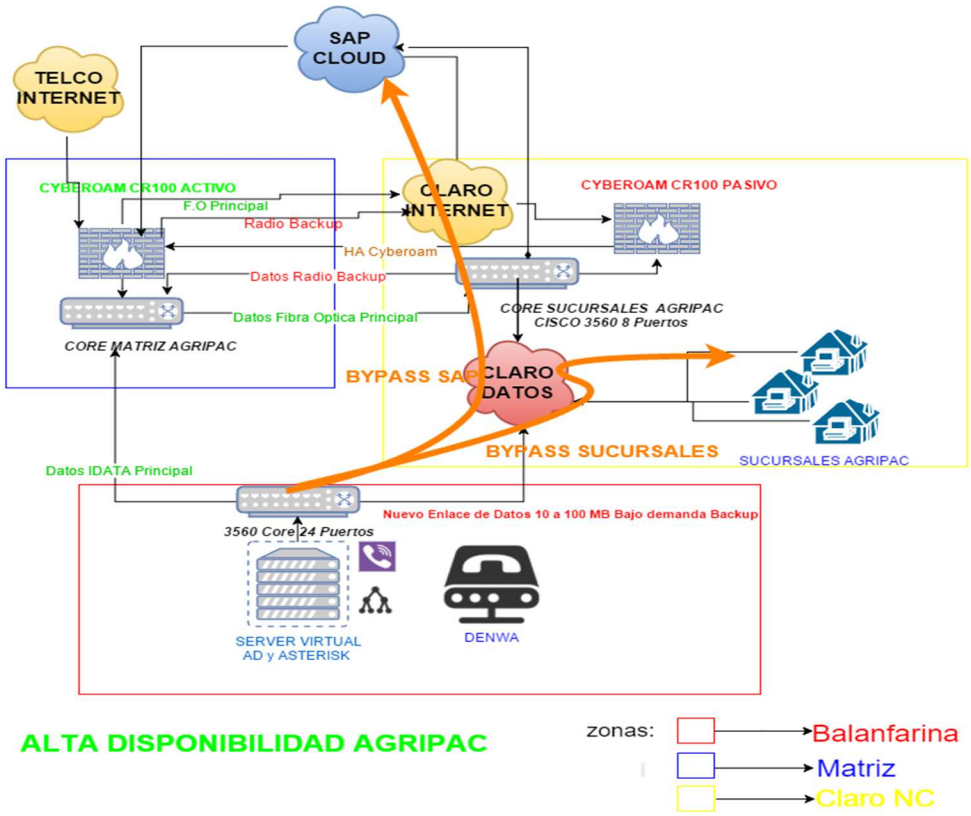


Figura 6.1 Conexiones con Alta Disponibilidad

Para el sistema ERP SAP al estar alojado en la Nube aseguramos su acceso mediante el servicio a internet y las políticas y configuraciones necesarias en el UTM:

UTM de alta disponibilidad ACTIVO/PASIVO

El UTM CR100 de backup (Pasivo) se configurara conjuntamente con el SWITCH de capa 3 para realizar los servicios de:

- NAT
- PORT FORWARDING
- WAF (Web Application Firewall)
- PROXY WEB
- PERMISOS
- ZONA DMZ
- AUTENTICACION

Se interconectara el CR100 de Matriz con el CR100 de Nuevo Carmen para tener una copia en caliente de las configuraciones y servicios provistos por el UTM es decir en el caso de la pérdida del UTM principal automáticamente el UTM Pasivo entra en funcionamiento manteniendo los servicios de Navegación de internet, Correos Gmail, etc.

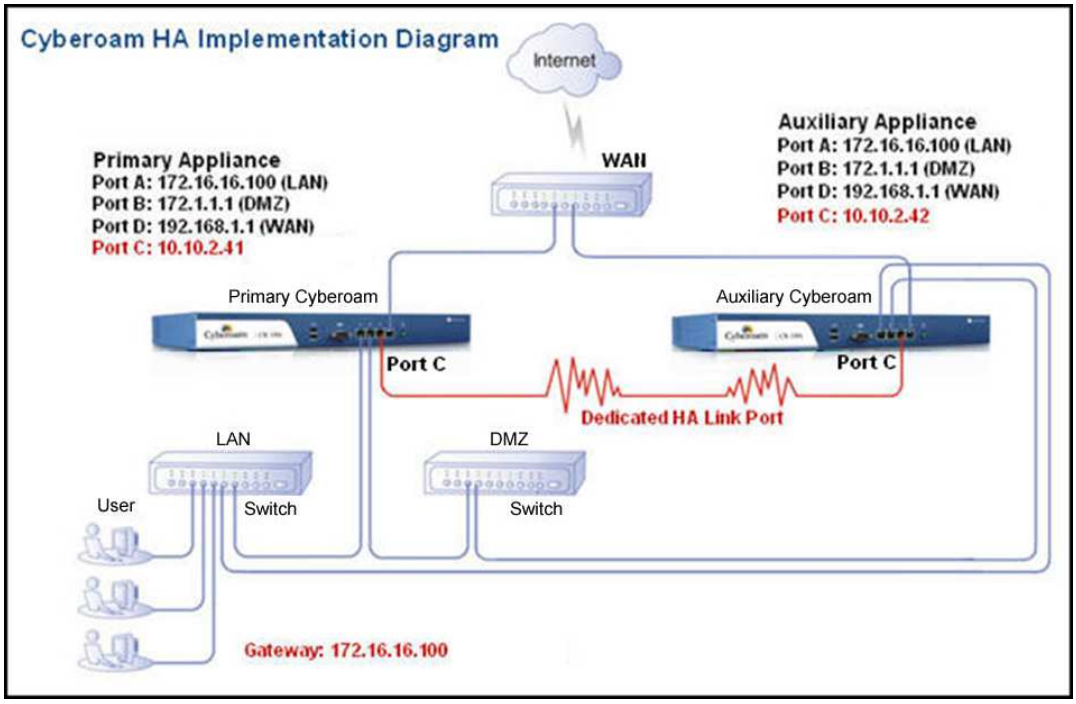


Figura 6.2 Diagrama de Implementación Cyberoam

Prueba de conectividad

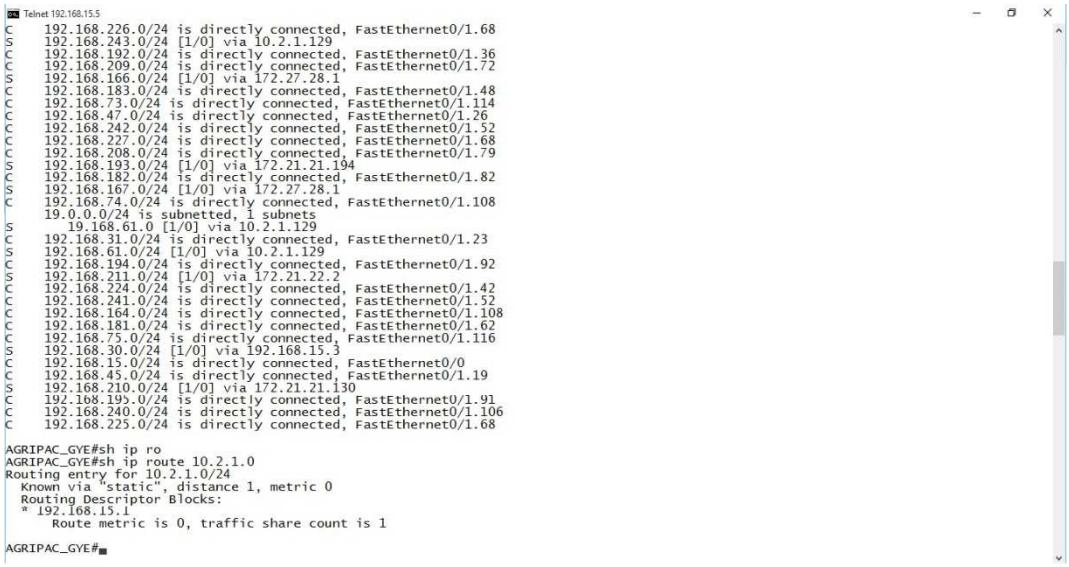


Figura 6.3 Pruebas de conectividad

Para la Nube del SAP pueden existir 2 tipos de conectividad:

- NUBE Publica (Publicada al Internet)
- NUBE Privada (Interconexión con la red de datos de Agripac)

REPLICA NUBE PRIVADA

En el caso de una nube privada la interconexión se debería realizar uniendo a L3 y Claro con un Crossconnect en Nuevo Carmen de esa forma Matriz no se convertiría en un único punto de fallo sino que tendríamos la alternativa de Balanfarina para la réplica de datos.

REPLICA NUBE PÚBLICA

Si la nube es publica el servicio de internet con el UTM en HA ubicado en la RBS de Claro nos asegura su acceso y replicación.

Para el acceso ininterrumpido de las conexiones a SAP existen 2 opciones:

1. Que la conexión a SAP sea realizada mediante Agripac Matriz, si es de esta manera la Nube del SAP será accesible mediante el switch de CORE de Matriz interconectado a la RBS de Claro en Nuevo Carmen.

2. Que la conexión a SAP sea mediante el Switch de Core Ubicado en Claro en Nuevo Carmen de esta manera el Switch de Core ahí instalado

mediante el OSPF realizaría un Bypass entre las sucursales y Balanfarina para dar acceso a SAP ya sea mediante enlace de Datos o Internet.

6.2 PRUEBAS DE ACTUALIZACIÓN DE INFORMACIÓN AL RESPALDO EN LA NUBE.

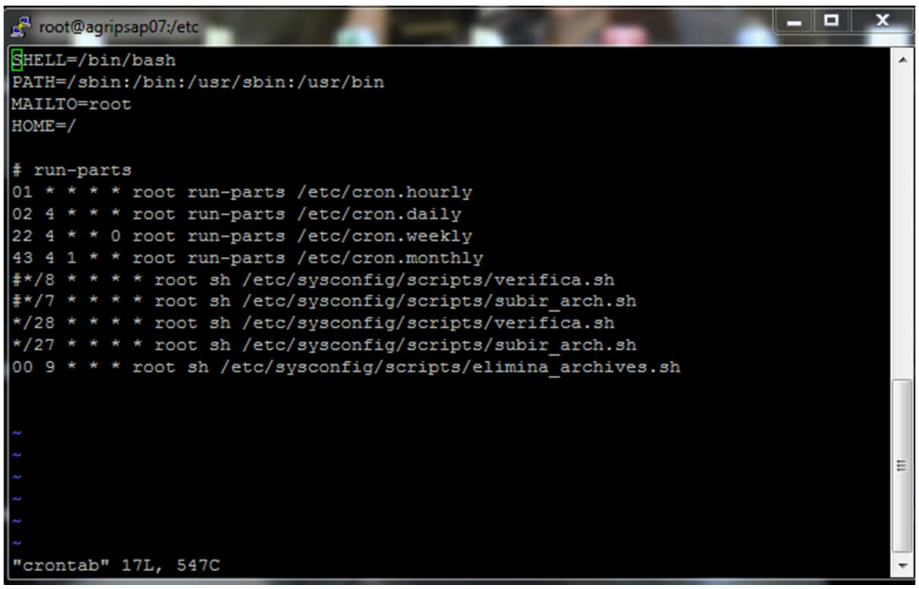


Figura 6.4 Definición de horarios y ejecución de actualización información a réplica

Una vez que se haya instalado el enlace que comunica con el data center del proveedor cuyo ancho de banda deberá ser de 10 Gbyte pero con opción de ser ampliado 30 Gbyte para cuando se requiera que pase de réplica a productivo y se haya instalado SAP, configurado el servidor de producción, se deberá proceder a migrar la base de datos a dicho servidor de réplica, luego se deberán realizar pruebas de actualización de

información en dicho servidor de backup o réplica ejecutando el siguiente proceso:

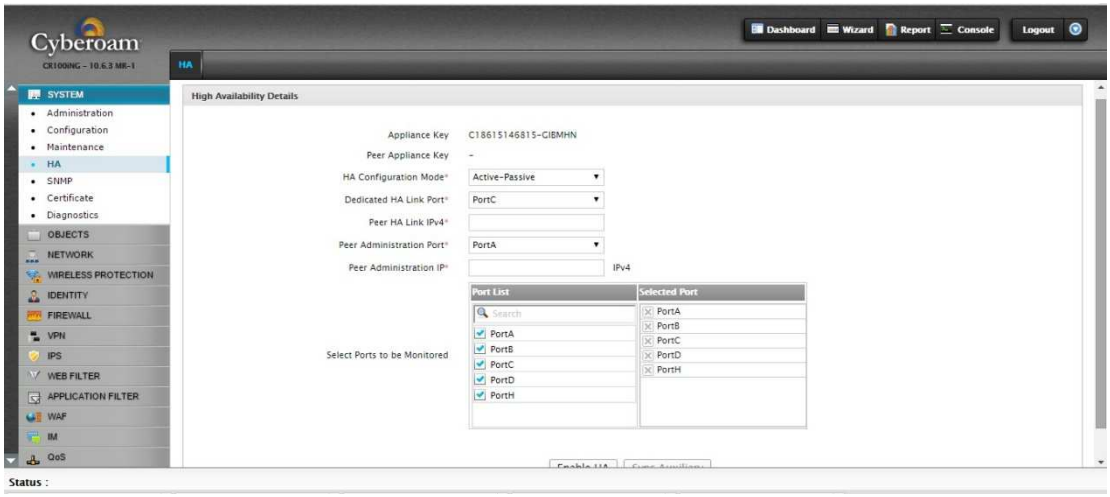


Figura 6.5 Detalle de Alta Disponibilidad con Cyberoam, con data center

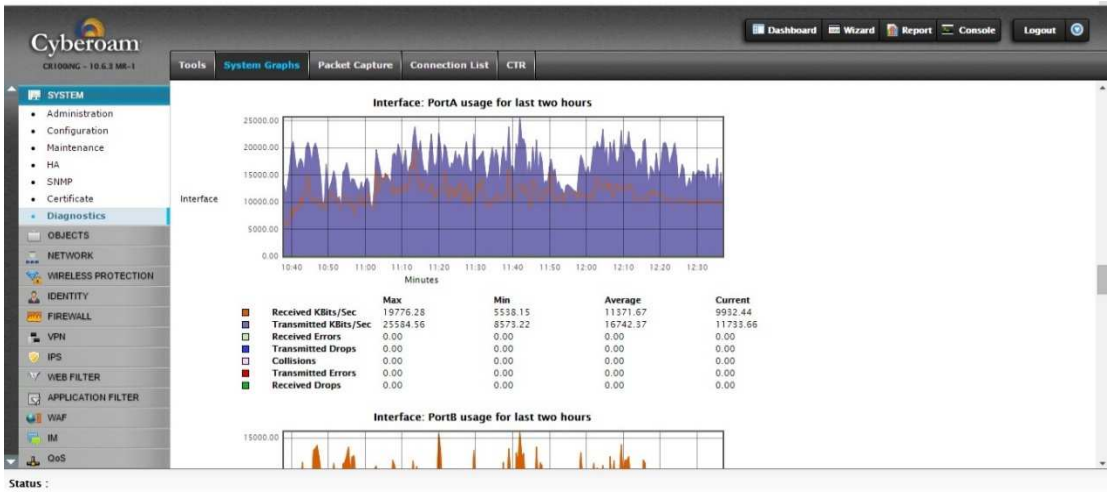


Figura 6.6 Sistema gráfico de diagnóstico conexión con data center.

6.3 PRUEBAS DE CONFIGURACIÓN DE ROUTERS Y PUNTOS DE RED EN CENTRO ALTERNO.

La configuración del router, de los puntos de red y del servidor de acceso se deberá ejecutar por separado para garantizar su adecuado funcionamiento tanto de acceso como de control de reglas y políticas de seguridad de la información.

```
RouterC(config-router)#router ospf 100
RouterC(config-router)#network 0.0.0.0 255.255.255.255 area 1
RouterC(config-router)#area 1 stub

RouterA(config-router)#router ospf 100
RouterA(config-router)#network 172.16.20.128 0.0.0.7 area 0
RouterA(config-router)#network 172.16.20.8 0.0.0.7 area 1
RouterA(config-router)#area 0 range 172.16.20.128 255.255.255.192
RouterA(config-router)#area 1 stub
RouterA(config-router)#area 1 default-cost 15

RouterE(config-router)#router ospf 100
RouterE(config-router)#network 172.16.20.144 0.0.0.7 area 0
RouterE(config-router)#area 1 stub
RouterE(config-router)#area 1 default-cost 30
RouterE(config-router)#area 0 range 172.16.20.128 255.255.255.192
```

Figura 6.7 Configuración de router centro alterno

Las pruebas deben incluir al SWITCH de capa 3 que deberá ser instalado en la Radio base de Nuevo Carmen para garantizar el enrutamiento desde el centro alterno al data center de la nube donde está alojado el servidor de réplica y/o producción, las pruebas también deberá incluir a otros elementos que son indispensables para el adecuado funcionamiento del centro alterno, estos son:

- ✓ Conexión local datos e internet CLARO (Puerto Ethernet)
- ✓ Servidor de control de accesos y contraseñas.
- ✓ Energía eléctrica ininterrumpida con UPS y Generador
- ✓ Aires acondicionados de precisión

De esta manera se convierte a nivel de enrutamiento a Matriz y a Balanfarina se convierten circuitos de Agencias Principales. En el caso de una caída hacia las 2 redes de servidores en matriz 10.2.1.0 y 10.1.1.0 el protocolo de enrutamiento redirigirá automáticamente este tráfico al data center de Backup en Balanfarina.

PROTOCOLO ENRUTAMIENTO.-

El tipo de enrutamiento que se utilizara será el OSPF creado también en zonas (Backbone, Matriz, Balanfarina) con el uso de este protocolo se obtienen los siguientes beneficios:

- ✓ Debido a las bases de datos de estados de enlaces sincronizados, los "router" OSPF convergerán mucho más rápido que los "routers" RIP tras cambios de topología. Este efecto se hace más pronunciado al aumentar el tamaño del AS.

✓ Incluye encaminamiento TOS ("Type of Service") diseñado para calcular rutas separadas para cada tipo de servicio. Para cada destino, pueden existir múltiples rutas, cada una para uno o más TOSs.

✓ Utiliza métricas ponderadas para distintas velocidades el enlace. Por ejemplo, un enlace T1 a.544 Mbps podría tener una métrica de 1 y un SLP a 9600 bps una de 10.

✓ Proporciona balanceo de carga ya que una ruta OSPF puede emplear varios caminos de igual coste mínimo.

✓ OSPF soporta rutas específicas de hosts, redes y subredes.

✓ OSPF permite que las redes y los hosts contiguos se agrupen juntos en áreas dentro de un AS, simplificando la topología y reduciendo la cantidad de información de encaminamiento que se debe intercambiar. La topología de un área es desconocida para el resto de las áreas.

El proceso se realizara de la siguiente manera, el proceso de enrutamiento y conexión principal es el enlace de datos que dirige su tráfico hacia el switch core en la red de Matriz esta vendría a ser la zona principal, La zona Backbone la delimitaremos a los equipos y redes de CLARO ya que este sería el discriminador del uptime de las zonas (Matriz/Balanfarina), en una zona Backup estaría la red de Balanfarina que al momento de detectar una caída (Parametrizable) en un corto tiempo restructurara su tabla de ruteo

haciendo Bypass a Matriz y conectando directamente a Balanfarina con las sucursales.

6.4 PRUEBAS DE DESVÍO DE ENLACES DE PLANTAS Y PUNTOS DE VENTAS DESDE BACKBONE DE PROVEEDOR AL CENTRO DE CÓMPUTO ALTERNO.

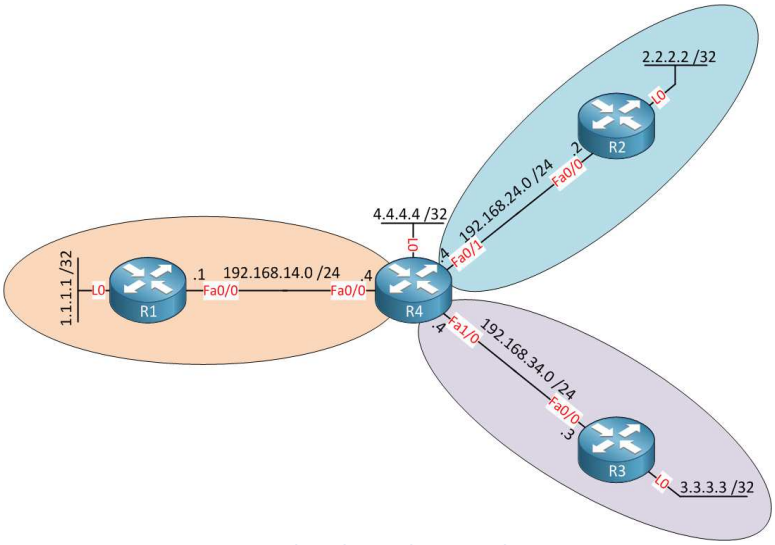


Figura 6.8 Enrutamiento de enlaces al centro alterno

```
ospf> enable
ospf# show ip ospf route
============ OSPF network routing table ============
N    10.10.10.0/24          [20] area: 0.0.0.0
                            via 10.103.4.222, PortB
N    10.103.4.0/24          [10] area: 0.0.0.0
                            directly attached to PortB
N    172.16.16.0/24         [10] area: 0.0.0.0
                            directly attached to PortA

============ OSPF router routing table =============

============ OSPF external routing table ============
```

Figura 6.9 Tabla de enrutamiento con OSPF

UTM de alta disponibilidad ACTIVO/PASIVO

El UTM CR100 de backup (Pasivo) se configurara conjuntamente con el SWITCH de capa 3 para realizar los servicios de:

- NAT
- PORT FORWARDING
- WAF (Web Application Firewall)
- PROXY WEB
- PERMISOS
- ZONA DMZ
- AUTENTICACION

Se interconectara el CR100 de Matriz con el CR100 de Nuevo Carmen para tener una copia en caliente de las configuraciones y servicios provistos por el UTM es decir en el caso de la pérdida del UTM principal automáticamente el UTM Pasivo entra en funcionamiento manteniendo los servicios de Navegación de internet, Correos Gmail, etc.

6.5 PRUEBAS DE ACCESO AL SERVIDOR DE RESPALDO DEL DATA CENTER DESDE EL CENTRO ALTERNO

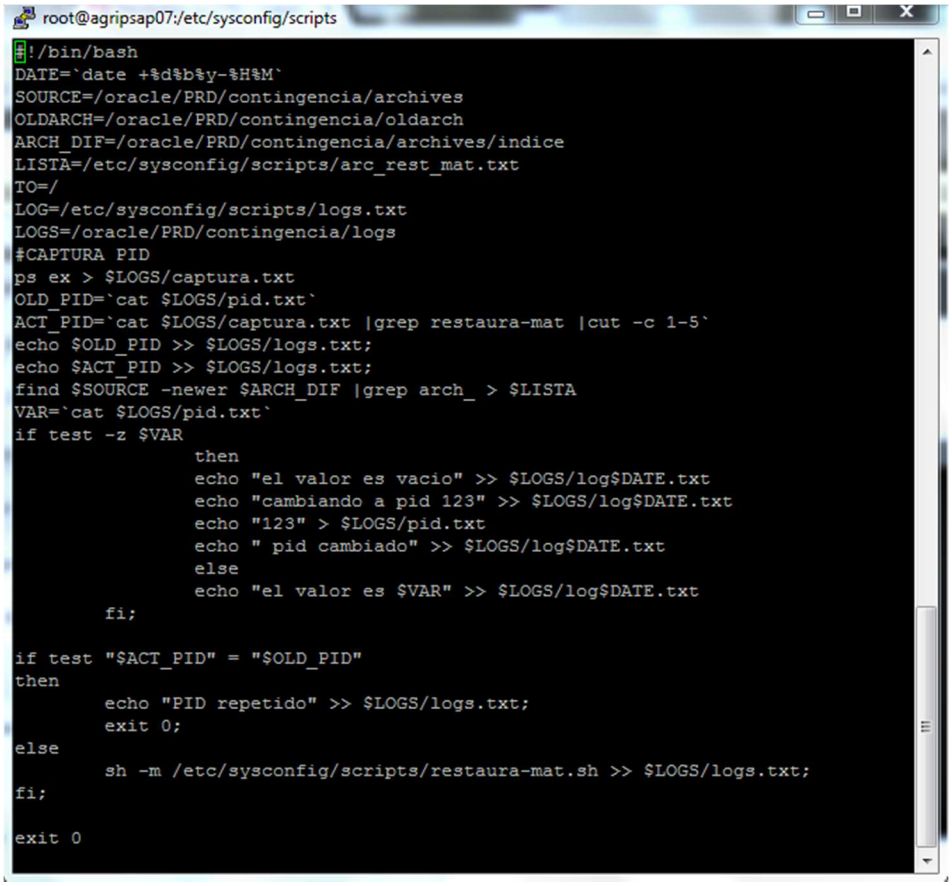


Figura 6.10 Prueba de acceso al servidor de producción en la nube desde el centro alterno

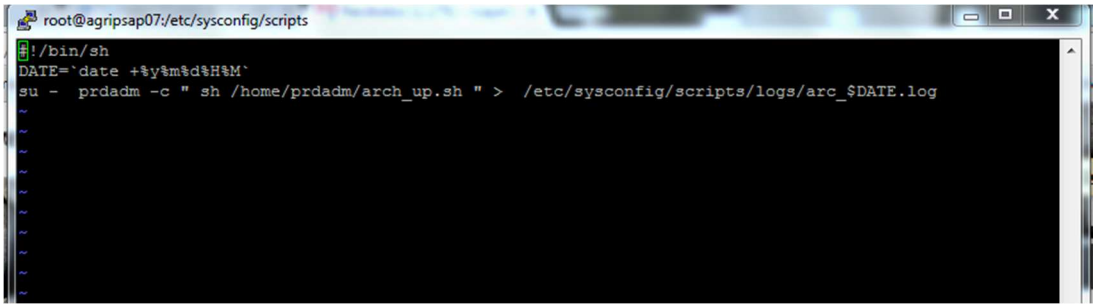


Figura 6.11 Verificación de carga al server del data center desde el centro alterno

Una vez realizadas satisfactoriamente las pruebas en el centro alterno de los routers, switch, puntos de red, enlaces de comunicaciones con el data center, se deberá coordinar con los proveedores de comunicaciones y del data center para cambiar el ruteo de los enlaces y el status del servidor de réplica a productivo.

Una vez habilitados dichos servicios se procederá a realizar las pruebas de accesos al servidor de producción en el data center.

Para el sistema ERP SAP al estar alojado en la Nube aseguramos su acceso mediante el servicio a internet y las políticas y configuraciones necesarias en el UTM (Control Unificada de Amenazas) se deberá utilizar un acceso mediante una nube privada integrada a la red de datos de Agripac.

Para la interconexión mediante una nube privada se unirá un L3 y Claro con un Crossconnect en Nuevo Carmen de esa forma Matriz no se

convertiría en un único punto de fallo sino que tendríamos la alternativa de Balanfarina para la réplica de datos.

Si la nube es publica el servicio de internet con el UTM en HA ubicado en la RBS de Claro nos asegura su acceso y replicación.

Para el acceso ininterrumpido de las conexiones a SAP existen 2 opciones:

Que la conexión a SAP sea realizada mediante Agripac Matriz, si es de esta manera la Nube del SAP será accesible mediante el switch de CORE de Matriz interconectado a la RBS de Claro en Nuevo Carmen.

Que la conexión a SAP sea mediante el Switch de Core Ubicado en Claro en Nuevo Carmen de esta manera el Switch de Core ahí instalado mediante el OSPF realizaría un Bypass entre las sucursales y Balanfarina para dar acceso a SAP ya sea mediante enlace de Datos o Internet.

Se deberá ubicar un servidor físico en Balanfarina el cual debe de ser instalado con un sistema operativo de Virtualización y dentro de su Hypervisor se crearan las siguientes Máquinas virtuales:

- Active Directory (3 Copia) 10.2.1.11 y 10.2.1.6
- DNS server
- WEB Services facturación electrónica

- Asterisk

En este servidor se deberá de configurar un Domain Controller de respaldo que contenga la copia activa de los servidores de dominio principales ubicados en Agripac Matriz estos servidores son el 10.2.1.11 y 10.2.1.6. Este nos servirá para mantener los login y autenticación de los usuarios ante la posible pérdida de los ubicados en Matriz.

El servidor deberá tener las siguientes características:

- ✓ 32 GB RAM
- ✓ Arreglo de Discos RAID 5 Discos SAS
- ✓ 1 o 2 Procesadores
- ✓ 4 NIC GigaEthernet

6.6 PRUEBA DE COMUNICACIONES ENTRE LOS EQUIPOS QUE INTEGRAN EL COMITÉ DE CONTINGENCIA.

Entre los equipos que integran el Comité de Contingencia debe existir permanente comunicación para que estén informados de cualquier novedad, comunicación o mejora que se le realice al plan de continuidad de negocio, se recomiendan los siguientes aspectos:

1. Todas las comunicaciones que emita el Comité de Contingencia sea difundido por correo aprovechando que todos los usuarios cuentan con el servicio de correo en sus Smartphone.
2. Crear un grupo de correo con los usuarios miembros del Comité de Contingencia, para que reciban las comunicaciones sobre el plan de continuidad de negocio.
3. Todos los usuarios del Comité deben tener acceso a la carpeta digital con toda la documentación que se encuentra alojada en el servidor que está en el centro alterno.
4. Dotar a los coordinadores de cada equipo de un radio de transmisión con largo alcance para garantizar que se puedan comunicar en caso de un desastre natural que deje fuera de servicio a los celulares.

6.7 PRUEBA INTEGRAL “SIMULACRO” DEL PLAN DE CONTINUIDAD DE NEGOCIO Y DE RECUPERACIÓN DE DESASTRE.

Los principales objetivos de la prueba o simulacro del Plan de Continuidad de Negocio y de Recuperación de Desastre son:

- Evaluar si el plan de continuidad de negocio funcionará.
- Verificar que los tiempos estimados para reanudar las actividades es mayor o menor al tiempo real.

- Documentar los procesos de la prueba y analizar las actividades que no se cumplieron para posterior a ello reestructurar el plan de Continuidad.

Antes de la realización de la prueba se debe convocar a los equipos, determinar la fecha y hora de la prueba y determinar el alcance de la misma, además se debe aplicar la siguiente lista de verificación:

Tabla 31 Calificación de las pruebas del BCP

1	Se capacitó al personal para responder a una emergencia	SI	NO
2	Se realizó el manual de funciones para el Comité de Contingencia	X	
3	Se cuenta con la información digital centralizada de los manuales y procedimientos para la contingencia	X	
4	La lista con los nombres, teléfonos y dirección de los usuarios claves y miembros de los equipos la tienen todos los miembros de los equipos.	X	
5	Se verificó que los enlaces con el centro alterno esté operativo	X	
6	Se coordinó con el proveedor de la nube la prueba	X	
7	Todos los miembros del equipo, proveedores de comunicaciones y data center conocen la fecha y hora de la prueba	X	
8	Se confirmó que en el centro alterno estén todos los recursos y materiales que se requieren para la prueba	X	

Una vez concluida la prueba o simulacro se deberá analizar los resultados y se debe otorgar una puntuación sobre las respuestas satisfactoria y su grado de cumplimiento, en base a ellos se proponen mejoras para las actividades que no funcionaron adecuadamente.

La mejor forma de saber si funcionó el Plan de Continuidad, es probando el funcionamiento de los procesos críticos y la integridad de los datos.

Una vez concluido el Plan de Continuidad de Negocio debe ser probado mediante un simulacro, el Comité de Contingencia deberá elaborar los formularios respectivos para dejar documentado la ejecución de cada una de las actividades así como los tiempos que tomó la ejecución del plan, la prueba o el simulacro permitirá detectar las fallas del plan y corregirlas, el siguiente formulario se debe aplicar en la prueba del plan.

Se emiten reportes con los resultados obtenidos

6.8 ANÁLISIS DE RESULTADOS

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.

Tabla 32 Pasos y Actividades del Comité de Contingencia

Paso	Actividades
1.	Comité de Contingencia se reúne y pide informe de daños a: a. Líder de Tecnología. b. Líder de Infraestructura. c. Líder de RRHH
2.	Comité de Contingencia decide declarar la contingencia en base a informe de daños.
3.	Equipo de Comunicaciones informa a los Líderes de cada equipo (se inicia árbol de llamadas), se prioriza la reunión del Comité de Contingencia.
4.	El líder de Tecnología comunica al proveedor del data center para que cambie el status del servidor de backup a productivo y que levante el aplicativo SAP.
5.	El líder de tecnología comunica a proveedor de comunicaciones cambiar ruteo de los enlaces hacia el data center de la nube y habilitar el enlace del centro alterno
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.	Administrador de Red y BASIS SAP habilitan el servidor del centro alterno y el acceso a la red para activar el ingreso de los diferentes equipos del Comité de Contingencia
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 de los procesos críticos en SAP.
10.	Líder de IT solicita al Equipo de Comunicaciones notificar a las Agencias y plantas que vuelvan a trabajar pero solo con los procesos críticos.

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

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

Administración y Mantenimiento del Plan de Continuidad de Negocio BCP y Recuperación de Desastre DRP

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.

CONCLUSIONES Y RECOMENDACIONES

Con la implementación de este Plan de Continuidad de Negocio y de Recuperación de Desastre, la empresa puede en un tiempo tolerable restablecer sus procesos críticos basados en las siguientes conclusiones:

1. **Conclusión:** La dirección y los usuarios claves de la empresa están motivados y concientizado de los beneficios del BCP, lo que garantiza su aplicación y ejecución casi de forma inmediata.

   Recomendación: Difundir el Plan en toda la organización.

2. **Conclusión:** El beneficio para la empresa de contar con este plan de Continuidad de Negocio, supera ampliamente el costo de su implementación, por lo tanto está plenamente justificada la inversión.

   Recomendación: Mantener operativos los recursos necesarios para la ejecución del plan en el centro alterno.

3. **Conclusión:** El proveedor del data center donde se alojará el servidor de backup, cuenta con las certificaciones TIER IV lo que garantiza la alta disponibilidad y operatividad del servicio.

   Recomendación: Mantener al día los contratos con los proveedores del data center y de comunicaciones.

4. **Conclusión:** El plan ha sido desarrollado para cubrir el peor escenario, por lo tanto que los escenarios de menor rango han quedado también cubiertos.

   Recomendación: Realizar mínimo una vez al año simulacro para garantizar el funcionamiento del Plan de Continuidad.

5. **Conclusión:** En conjunto con las diferentes áreas del negocio se analizaron y determinaron los elementos claves del negocio.

   Recomendación: Mantener actualizado los nombres, direcciones y teléfonos de los miembros de los diferentes equipos del Plan de Contingencia.

6. **Conclusión:** Se involucró a la alta gerencia así como a los responsables del área comercial y de producción.

   Recomendación: Nombrar a un responsable del equipo de Contingencia para que realice los mantenimientos del Plan.

BIBLIOGRAFÍA

[1] Plan para la Continuidad del Negocio (BCP y DRP), http://www.sisteseg.com/sin-dustrial.html, fecha de consulta diciembre 2015

[2] Sistemas Corporativos. Alta Disponibilidad, Continuidad de Negocio y entorno ante desastres, http://blog.edisa.com/2014/05/sistemas-corporativos-alta-disponibili-dad-continuidad-de-negocio-y-entorno-ante-desastres/, fecha de consulta diciem-bre 2015

[3] Evolución Actual de la Gestión de la Continuidad de Negocio: ISO 22301, http://www.eird.org/pr14/formulario/presentaciones/138.pdf, fecha de consulta di-ciembre 2015

[4] ISO 22301 Continuidad del Negocio - Metodología para la Implantación, https://eventioz.com.ar/e/iso-22301-continuidad-del-negocio-metodologia-para, fe-cha de consulta diciembre 2015

[5] ISO 22301: Beneficios, http://normaiso22301.com/que-beneficios-tiene-la-norma-iso-22301/, fecha de consulta diciembre 2015

[6] Primeros pasos con la norma ISO 22301: ISO 22301: Gestión de la Continuidad de Negocio, http://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/Re-quisitos-de-la-norma-ISO-22301/, fecha de consulta diciembre 2015

[7] Cloud SAP Datacenter, http://www.datacenter.cm/venezuela/es/cloud-sap-data-center.php, fecha de consulta diciembre 2015

[8] Manero Jaume, Ventajas de utilizar servicios Cloud para entornos SAP: rapidez, simplificación y flexibilidad, http://sapforummadrid2015.com/presentaciones/in-nova/Servicios_Cloud_para%20entornos_SAP_Jaume_Manero.pdf, fecha de con-sulta diciembre 2015

[9] Cómo hacer un Plan de Continuidad de Negocios (BCP) [II], http://blog.segu-info.com.ar/2014/09/como-hacer-un-plan-de-continuidad-II.html, fecha de consulta diciembre 2015

[10] British Standards Institution, Talking Business Continuity, http://www.talkingbusi-nesscontinuity.com, fecha de consulta noviembre 2015

[11] Ortiz Yuri Eide y Valeria Marcelo, Continuidad del negocio y una oportunidad para enfrentar desastres de las empresas chilenas, http://www.scribd.com/doc/27876103/Paper-Business-Continuity-Rev4, fecha de consulta noviembre 2015

[12] Business Continuity and Disaster Recovery, http://www.bcm-insti-tute.org/bcmi10/en/about-us, fecha de consulta diciembre 2015

[13] ISO 22301: Gestión de la Continuidad de Negocio, http://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio, fecha de consulta diciembre 2015

[14] Elaboración del Marco Teórico Tesis, http://www.monografias.com/trabajos94/elaboracion-del-marco-teorico-tesis/elaboracion-del-marco-teorico-tesis.shtml#ixzz3IFpp0Art, fecha de consulta diciembre 2015

[15] Gestión Continuidad Negocio en cuatro pasos, http://www.welivesecurity.com/la-es/2014/05/14/gestion-continuidad-negocio-cuatro-pasos, fecha de consulta diciembre 2015

GLOSARIO

Análisis de impacto del negocio (BIA)	BIA es la actividad de la gestión de la continuidad del negocio que identifica las funciones vitales del negocio y sus dependencias. Estas dependencias pueden incluir proveedores, personas, otros procesos de negocio, servicios TI, etc. BIA define los requerimientos de recuperación para los servicios de TI. Dichos requerimientos incluyen objetivos de tiempos de recuperación, objetivos del punto de recuperación y los objetivos mínimos de nivel de servicio para cada servicio de TI.
Copia de seguridad	Copiar los datos para proteger los originales de pérdidas de integridad o disponibilidad.
Disponibilidad	Habilidad de un elemento de configuración o de un servicio de TI para realizar las funciones acordadas cuando se requiere. La disponibilidad la determinan la fiabilidad, la

	mantenibilidad, el compromiso de servicio, el rendimiento y la seguridad.
Evaluación	Inspección y análisis para verificar si se está siguiendo un estándar o un conjunto de guías, que sus registros son precisos, o que se están cumpliendo las metas de eficiencia y efectividad.
Gestión de accesos	Proceso responsable de permitir a los usuarios hacer uso de los servicios de TI, datos u otros activos.
Gestión de eventos	Proceso responsable de la gestión de eventos a lo largo de su ciclo de vida. La gestión de ventas es una de las principales actividades dela operación de TI.
Gestión de crisis	El proceso responsable de gestionar las implicaciones más amplias de la continuidad de negocio. Un equipo de gestión de crisis es responsable de temas estratégicos tales como la gestión de los medios y de la confianza de los accionistas y decide cuándo invocar los planes de continuidad de negocio.

Gestión de la continuidad del negocio (BCM)	Es el proceso de negocio responsable de gestionar el riesgo que puede tener un alto impacto en el negocio. BCM protege los intereses de los principales interesados, la reputación, la marca y las actividades que aportan valor al negocio.
Plan de disponibilidad	Plan para asegurar que se puede proveer los requerimientos de disponibilidad actuales y futuros de los servicios TI de forma rentable.
Plan de la Continuidad del Negocio	Plan que define los pasos que se requieren para el restablecimiento de los procesos de negocio después de una interrupción. El plan también identifica los disparadores para la Invocación, las personas involucradas, las comunicaciones, etc. El plan de la continuidad del servicio de TI es una parte importante de los planes de continuidad del negocio.
Proveedor de servicios de internet (ISP)	Un proveedor externo de servicio que proporciona acceso a Internet. La mayoría de los ISP proporcionan también otros servicios de TI, tales como hosting de páginas web.

Tiempo acordado para el servicio (AST)	Sinónimo de horario del servicio, se usa frecuentemente en el cálculo de la disponibilidad.
Tolerancia a fallos	Habilidad de un servicio de TI o de un elemento de configuración para continuar su operación correcta tras el fallo de un componente.

ANEXOS

CLASIFICACIÓN PARA LA MATRIZ DE RIESGO INSTITUCIONAL

Tabla 33 Clasificación Matriz de Riesgo Institucional

TIPOS PERDIDA	
CÓDIGO	**DESCRIPCIÓN**
TP-01	Pérdida Económica
TP-02	Imagen Institucional
TP-03	Disponibilidad del servicio
TP-04	Multas de Organismos de control
TP-05	Confiabilidad
TP-06	Integridad de información
TP-07	Fuga de información
TP-08	Confidencialidad
TP-09	Reclamo de usuarios

CAUSAS DEL RIEGO	
CÓDIGO	**DESCRIPCIÓN**
CR-01	Procesos
CR-02	Personas
CR-03	Tecnologías

PROBALIDAD DEL RIESGO	
NRO.	**DESCRIPCIÓN**
1	Por lo menos 1 vez cada 5 años
2	Por lo menos 2 vez cada 3 años
3	Por lo menos 1 vez cada año
4	Por lo menos 2 veces cada año
5	1 vez cada mes

IMPACTO DEL RIESGO	
NRO.	**RANGO PERDIDA – USD**
1	0 - 30.000
2	30.001 - 100.000
3	100.001 - 500.000
4	500.00 - 800.000
5	Patrimonio de la empresa

Nro. Entrevista-dos	4

MATRIZ DE RIESGO OPERACIONAL

Tabla 34 Matriz de Riesgo Operacional

N.	TIPO DE PERDIDA	EVENTO DE RIESGO	CONTROLES ACTUALES	FACTOR DE RIESGO	AFECTACIÓN
1	Disponibilidad del servicio	Fallo en el Funcionamiento de la aplicación SAP	Contrato Mantenimiento con proveedor	- Tecnología	- Paralización general de la operatividad de la empresa
2	Disponibilidad del servicio	Interrupción de las comunicaciones con las Plantas y Puntos de Ventas	Enlaces principales redundantes	- Personas - Tecnología	- Tiempo prolongado sin prestar servicio a los usuarios.
3	Disponibilidad del servicio	Corte de energía prolongado	UPS-Generador eléctrico	- Personas - Tecnología	- Tiempo prolongado sin prestar servicio a los usuarios.
4	Disponibilidad del servicio	Manipulación de la infraestructura de sistemas	Control de acceso físico	- Personas - Tecnología	- Cierre temporal de instalaciones.
5	Disponibilidad del servicio	Suspensión del servicios de proveedor de internet	Enlaces redundante con otro proveedor	- Tecnología	- Tiempo prolongado sin prestar servicio a los usuarios.
6	Disponibilidad del servicio	Incendio en el edificio del Centro de Cómputo	Sistema contra incendio, personal preparado evacuación	- Personas	- Paralización general de la operatividad de la empresa
7	Disponibilidad del servicio	Atentado Terrorista que afecte el centro Cómputo	- Sistema de cámaras de vigilancia.	- Personas	- Paralización general de la operatividad de la empresa
8	Fuga de información	Robo de la información	Control de accesos físico y lógico	Personas tecnología	Pérdidas de activos de la empresa

9	Disponibilidad del servicio	Pérdida de conexión de la red	segmentación de red	- Personas - Tecnología - Procesos	- Tiempo prolongado sin prestar servicio a los usuarios.
10	Integridad de información	Daño o pérdida de información por ataque informático	- Implementación de políticas de navegación y control de acceso a internet.	- Personas - Tecnología	- Tiempo prolongado sin prestar servicio a los usuarios.
11	Integridad de información	Manipulación sensible sin autorización	Control de accesos y perfiles x cargos	Personas tecnología	- Perdida información. - Indisponibilidad de servicios.
12	Integridad de información	Error en programa de aplicativo	Control de modificaciones y pruebas de calidad	- Personas - Procesos	- Insatisfacción en el usuario funcional.
13	Integridad de información	Falla de la base de datos	backup y réplica	- Personas - Procesos	Interrupción de los servicios
14	Pérdida Económica	Pérdida x sustracción de contraseña	Política de caducidad de contraseñas	- Personas - Tecnología	- Registro incorrecto de la información.
15	Imagen Institucional	Vencimiento de licencias de aplicativos	Contrato de licencias vigentes	- Personas	- Multas y sanciones de organismos de control. - Pérdidas económicas para la empresa.

FORMULARIO DE ENTREVISTAS DE EVALUACION DE RIESGOS PARA AGRIPAC S. A.

Nombre: **Ing. Gustavo Wray**

Cargo: **Gerente General**

Departamento: **Gerencia General**

NRO.	EVENTO DE RIESGO	RIESGO INHERENTE		CONTROLES ACTUALES	RIESGO RESIDUAL		RIESGO RESIDUAL DESEADO	
		PROBABILIDAD	IMPACTO		PROBABILIDAD	IMPACTO	PROBABILIDAD	IMPACTO
1	Fallo en el Funcionamiento de la aplicación SAP	4	3	- No hay control.	5	3	2	1
2	Interrupción de las comunicaciones con las Plantas y Puntos de Ventas	5	4	Si hay control	3	2	2	1
3	Corte de energía prolongado	4	3	Si hay control	4	2	1	1
4	Manipulación de la infraestructura de sistemas	5	5	Si hay control	3	2	2	2
5	Suspensión del servicios de proveedor de internet	4	4	Si hay control	3	3	2	1
6	Incendio en el edificio del Centro de Cómputo	4	5	No hay control	4	4	2	2
7	Atentado Terrorista que afecte el centro Cómputo	4	5	No hay control	3	3	1	2
8	Robo de la información	4	4	Si hay control	2	3	2	1
9	Pérdida de conexión de la red	5	3	No hay control	3	3	2	2

10	Daño o pérdida de información por ataque informático	5	4	No hay control	4	2	3	1
11	Manipulación sensible sin autorización	3	5	Si hay control	3	3	2	1
12	Error en programa de aplicativo	3	4	Si hay control	4	3	3	2
13	Falla de la base de datos	4	5	Si hay control	4	4	2	3
14	Pérdida o sustracción de contraseñas	5	4	Si hay control	3	4	3	2
15	Vencimiento de licencias de aplicativos	3	3	Si hay control	3	3	2	2
16								

FORMULARIO DE ENTREVISTAS DE EVALUACION DE RIESGOS PARA AGRIPAC S. A.

Nombre: **Ec. Manuel Suco**

Cargo: **Contralor General**

Departamento: **Contralo-ría**

NRO.	EVENTO DE RIESGO	RIESGO INHERENTE		CONTROLES ACTUALES	RIESGO RESIDUAL		RIESGO RESIDUAL DESEADO	
		PROBA-BILIDAD	IMPACTO		PROBABILI-DAD	IMPACTO	PROBABILIDAD	IM-PACTO
1	Fallo en el Funcionamiento de la aplicación SAP	4	4	Si hay control	4	2	1	1
2	Interrupción de las comunicaciones con las Plantas y Puntos de Ventas	4	3	No hay control	4	3	1	2
3	Corte de energía prolongado	2	4	Si hay control	3	2	3	2
4	Manipulación de la infraestructura de sistemas	3	4	Si hay control	2	1	2	1
5	Suspensión del servicios de proveedor de internet	3	2	No hay control	4	3	3	2
6	Incendio en el edificio del Centro de Cómputo	5	5	No hay control	3	4	2	2
7	Atentado Terrorista que afecte el centro Cómputo	5	4	No hay control	4	3	3	1
8	Robo de la información	4	3	No hay control	3	4	4	2
9	Pérdida de conexión de la red	4	4	No hay control	3	2	3	2
10	Daño o pérdida de información por ataque informático	5	5	No hay control	3	3	2	1
11	Manipulación sensible sin autorización	4	3	Si hay control	4	2	3	2
12	Error en programa de aplicativo	4	2	Si hay control	3	3	2	1
13	Falla de la base de datos	4	5	Si hay control	4	2	2	2
14	Pérdida o sustracción de contraseñas	3	2	Si hay control	4	3	2	1
15	Vencimiento de licencias de aplicativos	2	2	Si hay control	4	2	1	1
16								

FORMULARIO DE ENTREVISTAS DE EVALUACION DE RIESGOS PARA AGRIPAC S. A.

Nombre: **Ing. Héctor Díaz**

Cargo: **Subgerente Sistemas y Comunicaciones**

Departamento: **Tecnología**

NRO.	EVENTO DE RIESGO	RIESGO INHERENTE		CONTROLES ACTUALES	RIESGO RESIDUAL		RIESGO RESIDUAL DESEADO	
		PROBABILIDAD	IMPACTO		PROBABILIDAD	IMPACTO	PROBABILIDAD	IMPACTO
1	Fallo en el Funcionamiento de la aplicación SAP	4	3	Si hay control	3	3	2	2
2	Interrupción de las comunicaciones con las Plantas y Puntos de Ventas	3	2	No hay control	4	3	2	1
3	Corte de energía prolongado	3	3	Si hay control	3	2	3	1
4	Manipulación de la infraestructura de sistemas	3	3	Si hay control	3	1	3	1
5	Suspensión del servicios de proveedor de internet	2	3	No hay control	4	2	2	2
6	Incendio en el edificio del Centro de Cómputo	5	4	No hay control	3	3	3	1
7	Atentado Terrorista que afecte el centro Cómputo	4	5	No hay control	4	3	3	1
8	Robo de la información	3	4	No hay control	4	3	3	2
9	Pérdida de conexión de la red	3	3	No hay control	2	3	2	2
10	Daño o pérdida de información por ataque informático	4	4	No hay control	3	4	2	1
11	Manipulación sensible sin autorización	4	3	Si hay control	4	2	2	2
12	Error en programa de aplicativo	3	4	Si hay control	3	3	2	1
13	Falla de la base de datos	3	4	Si hay control	4	2	2	2
14	Pérdida o sustracción de contraseñas	3	3	Si hay control	4	3	2	1
15	Vencimiento de licencias de aplicativos	2	2	Si hay control	4	2	1	1
16								

FORMULARIO DE ENTREVISTAS DE EVALUACION DE RIESGOS PARA AGRIPAC S. A.

Nombre: **Ing. Bolívar Vallejo**

Cargo: **Gerente de Sistemas TI**

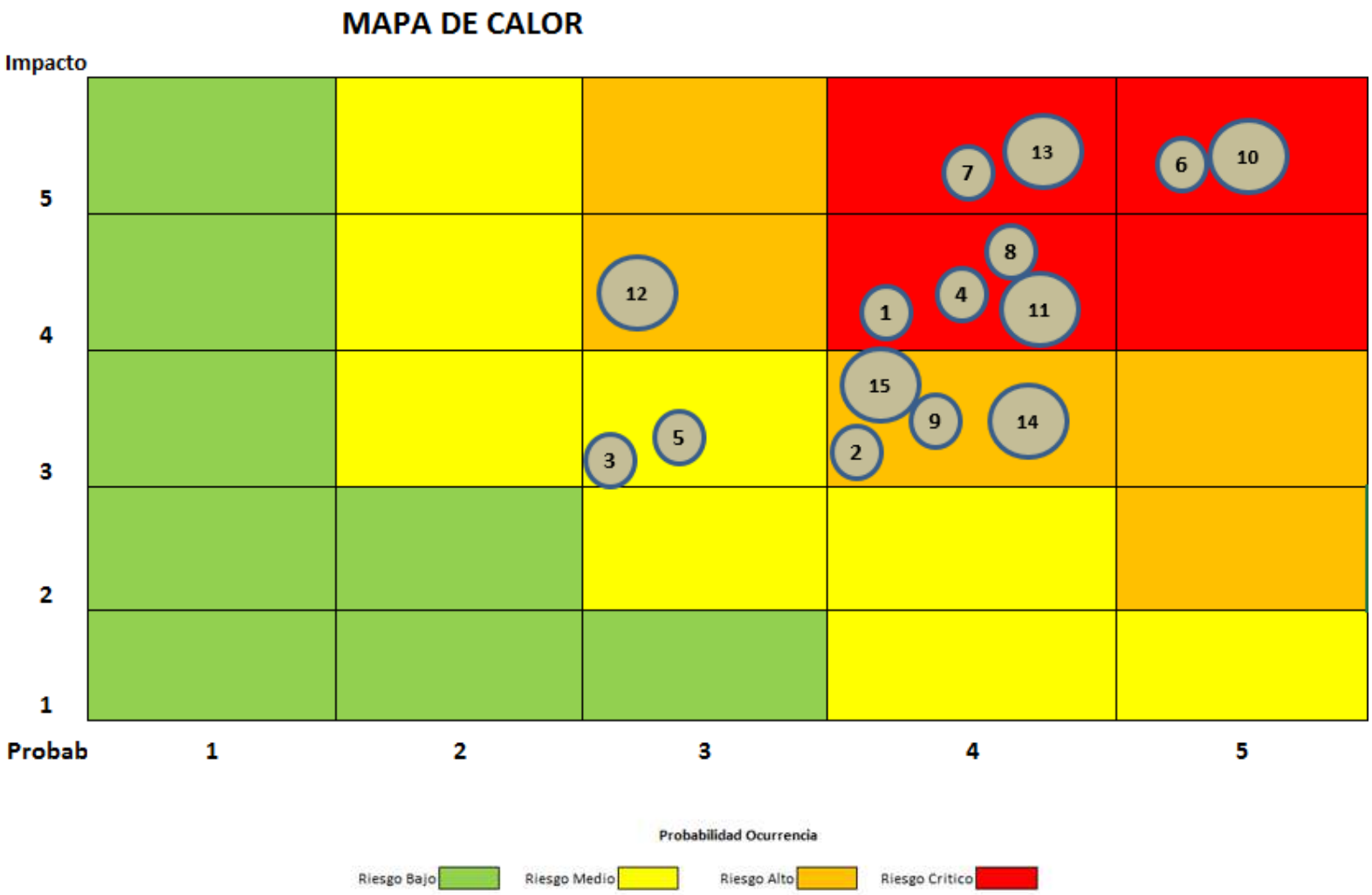
Departamento: **Departamento de Tecnología**

NRO.	EVENTO DE RIESGO	RIESGO INHERENTE		CONTROLES ACTUALES	RIESGO RESIDUAL		RIESGO RESIDUAL DESEADO	
		PROBABILIDAD	IMPACTO		PROBABILIDAD	IMPACTO	PROBABILIDAD	IMPACTO
1	Fallo en el Funcionamiento de la aplicación SAP	3	4	No hay control.	3	3	2	2
2	Interrupción de las comunicaciones con las Plantas y Puntos de Ventas	4	3	Si hay control	4	2	1	1
3	Corte de energía prolongado	4	3	Si hay control	3	2	2	1
4	Manipulación de la infraestructura de sistemas	3	4	Si hay control	3	2	1	2
5	Suspensión del servicios de proveedor de internet	4	3	Si hay control	3	3	2	1
6	Incendio en el edificio del Centro de Cómputo	4	5	No hay control	3	4	1	2
7	Atentado Terrorista que afecte el centro Cómputo	3	5	No hay control	3	3	1	2
8	Robo de la información	3	4	Si hay control	3	2	2	1
9	Pérdida de conexión de la red	4	3	No hay control	3	4	2	2
10	Daño o pérdida de información por ataque informático	4	4	No hay control	4	2	3	1
11	Manipulación sensible sin autorización	3	5	Si hay control	3	3	2	1
12	Error en programa de aplicativo	3	4	Si hay control	4	3	3	2
13	Falla de la base de datos	3	5	Si hay control	4	4	2	3
14	Pérdida o sustracción de contraseñas	4	4	Si hay control	3	4	3	2
15	Vencimiento de licencias de aplicativos	3	3	Si hay control	3	3	2	2

Matriz de Evaluación

NRO.	EVENTO DE RIESGO	RIESGO INHERENTE		CONTROLES ACTUALES	RIESGO RESIDUAL		RIESGO RESIDUAL DESEADO	
		PROBABILIDAD	IMPACTO		PROBABILIDAD	IMPACTO	PROBABILIDAD	IMPACTO
1	Fallo en el Funcionamiento de la aplicación SAP	4	4	No hay control.	5	3	2	1
2	Interrupción de las comunicaciones con las Plantas y Puntos de Ventas	4	3	Si hay control	3	2	2	1
3	Corte de energía prolongado	3	3	Si hay control	4	2	1	1
4	Manipulación de la infraestructura de sistemas	4	4	Si hay control	3	2	2	2
5	Suspensión del servicios de proveedor de internet	3	3	Si hay control	3	3	2	1
6	Incendio en el edificio del Centro de Cómputo	5	5	No hay control	4	4	2	2
7	Atentado Terrorista que afecte el centro Cómputo	4	5	No hay control	3	3	1	2
8	Robo de la información	4	4	Si hay control	2	3	2	1
9	Pérdida de conexión de la red	4	3	No hay control	3	3	2	2
10	Daño o pérdida de información por ataque informático	5	5	No hay control	4	2	3	1
11	Manipulación sensible sin autorización	4	4	Si hay control	3	3	2	1
12	Error en programa de aplicativo	3	4	Si hay control	4	3	3	2

13	Falla de la base de datos	4	5	Si hay control	4	4	2	3
14	Pérdida o sustracción de contraseñas	4	3	Si hay control	3	4	3	2
15	Vencimiento de licencias de aplicativos	3	3	Si hay control	3	3	2	2


MAPA DE CALOR
Impacto
5
4
3
2
1
Probab
1
2
3
4
5
13
7
6
10
8
12
4
1
11
15
9
14
5
3
2
Probabilidad Ocurrencia
Riesgo Bajo
Riesgo Medio
Riesgo Alto
Riesgo Critico

PROCEDIMIENTOS DE RECUPERACIÓN

RECURSOS MÍNIMOS DE RECUPERACIÓN

CARGO	NOMBRE	FUNCIÓN
Líder de Sistemas	Bolívar Vallejo	Responsable del correcto funcionamiento del centro de cómputo alterno, 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 y comunicaciones	Carlos Suárez	Responsable del correcto funcionamiento de red LAN y de las redes WAN, así como las comunicaciones con las plantas, puntos de ventas e Internet

Especialista en Base de Datos Y sistema Operativo LINUX RED HAT, BASIC-SAP	R. Cayetano	Encargado de controlar que la base de datos del servidor de replicación funcione adecuadamente y se mantenga actualizada
Responsable del ambiente de Producción y custodia de los códigos fuentes	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 Funcionamiento módulos de SAP	Manolo Viera	Coordinar con los consultores funcionales, Roles y Perfiles, el correcto funcionamiento del ERP.SAP

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 alterno, los que detallamos a continuación.

EQUIPO DE RECURSOS HUMANOS PARA OPERAR EL CENTRO DE CÓMPUTO ALTERNO

Inventario de Activos del Centro de Computo Alterno

EQUIPO	CARACTERISTICAS	IDENTIFICACION
15 Laptops DELL I5	Procesador Intel I5 4 RAM 1 TB Disco, puerto HDMI, USB	AGH-001
1 Routers Cisco Catalyst	Modelo 3560	AGH-002
1 UPS marca Best Power On Line	3 KVA On Line	AGH-003
2 Switch Marca CISCO Catalyst	Modelo 2960 100 Mb 24 P	AGH-004
3 Impresoras	Laser de 18 ppm	AGH-008
1 UTM	Cyberoam	2100
10 Líneas de Telefono	Digitales de Pacifictel	AGH-006
1 Copiadora	Xérox	AGH-007

1 Asterist Voz IP		
20 Teléfonos IP Cisco		
20 cables de red		
20 mouses		
10 Monitores	HDMI	
10 Monitores	SVGA	

INVENTARIO DE HARDWARE DE COMUNICACIONES DEL PROVEEDOR

EQUIPO / ENLACE	UBICACION	CARACTERISTICAS TECNICAS
Switch 3560	RBS Nuevo Carmen	**CISCO Catalyst 3560** **8** Puertos 10/100/1000 con IOS de Cisco Advance IP services
UTM Cyberoam	RBS Nuevo Carmen	**Cyberoam,CR100iNG** 8 Copper GbE Ports, Configurable Internal/DMZ/WAN Ports, WRR based- Automated Failover/Failback trunking),VLAN,WWAN,TAP -DynamicRouting:RIPv1&v2,OSPF,BGP,PIM-SIM,Modulo WAF (Web Services)
Switch 3560	Balanfarina	**CISCOCatalyst3560 24** Puertos 10/100/1000 con IOS de Cisco Advance IP services
Servidor HP	Balanfarina	**HPProliantDL360Gen9** SAS/SATA/SSDSFF Controlador de red Adaptador Ethernet 331i de 1 Gb 4 puertos por controlador y/o Memoria32GBFamiliadeproductosIntel®Xeon®E5-2600v3Númerodeprocesadores2Núcleo de procesador disponible 18
Denwa Central IP	Balanfarina	ProcesadorInteli33240, Sistema Operativo Linux, Memoria4GbDDR3, Almacenamiento interno sistema 120 GB SSD, almacenamiento interno 1 tb Serial ATA, Red RED Dual Gigabyte Ethernet.
Enlace de Datos on Demand	RBS Nuevo Carmen / Balanfarina	**Enlace de Datos Corporativo** 10MBBajoDemandaInterfazdeconexiónEthernetClear channel de capa 2

INVENTARIO DE SOFTWARE DEL CENTRO DE CÓMPUTO ALTERNO

SOFTWARE	CARACTERISTICAS	IDENTIFICACION
1 Licencia de Linux Red Hat	Versión 5.18	AGS-001
5 Licencia de Linux Red Hat	Versión 5.18	AGS-002
30 Licencia SAP DBA	Versión 11.5	AGS-003
	Versión 7.23	AGS-004
Software aplicativo integrado SAP	Versión 6.0.2 R	AGS-005
	Versión 2003	AGS-006
10 Licencias Antivirus Kaspersky	Versión 2003	AGS-007
10 licencias Antivirus 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

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.

PROCEDIMIENTO DE MODIFICACIONES EN PROGRAMA SAP

FP.INF.002-04_____

AGRIPAC S.A.

Sistemas y Comunicaciones

FICHA TECNICA DE MODIFICACIONES

FECHA	:	PRIORIDAD	:
COMPAÑIA	:	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

FP.INF.002-04

Observación:_____

_____

_____

Analista Responsable

Gerencia de Sistemas

PROCEDIMIENTO DE MANTENIMIENTO DE HARDWARE Y SOFTWARE

PR-INF-004

PROCEDIMIENTO DE MANTENIMIENTO PREVENTIVO DE HARDWARE Y SOFTWARE DE ESTACIONES DE TRABAJO

Revisión: 03

Fecha de vigencia: Abril 01 del 2014

CONTROL DE CAMBIOS		
Revisión	**Hojas Afectadas**	**Causa**
02	**TODAS**	**INCLUSION DEL MANTENIMIENTO DE SOFTWARE**
RUTA DE APROBACION		
Función	**Nombre**	**Cargo**
Elaborado	Jennifer Barrera	Asistente de Gerencia
Revisado y Aprobado	Bolívar Vallejo	Gerente de Sistemas

Realizar los mantenimientos preventivos de los servidores y estaciones de trabajo incluyendo impresoras y demás hardware que complementan las estaciones de trabajo de todos los usuarios de la organización lo que permitirá garantizar el normal funcionamiento de estas indispensables herramientas de trabajo y que el personal involucrado en los procesos de mantenimiento preventivo y correctivo tenga un documento que les facilite ésta actividad.

Alcance

Este proceso de mantenimiento preventivo y correctivo cubre todos los servidores y estaciones de trabajo del Grupo Corporativo (Hardware y Software) incluyendo los que están en los puntos de ventas remotos, se inicia con la planificación y finaliza con la emisión y firma por parte del usuario del registro de mantenimiento realizado, o un correo que quede como constancia del mismo, cuyo responsable del envío será el técnico a cargo. Los mantenimientos preventivos deberán ser programados en los meses de bajo movimientos para evitar interrupción de las normales actividades de la empresa.

Para la elaboración de este documento consideraron los criterios establecidos en:

- Manual del Sistema de Gestión Integrado.
- Procedimiento PR-SGI-002 Control de Documentos
- Plantilla 001 Procedimientos

- **Servidor:** Es un computador con mayor recurso y alta capacidad de procesamiento que permite almacenar una o varias aplicaciones informáticas o programas que realizan algunas tareas específicas.
- **Aplicación Informática:** Un conjunto de programas e instrucciones que permiten procesar transacciones y obtener información para un determinado objetivo.

Todas las computadoras y demás hardware deberán tener un mantenimiento por lo menos una vez al año.

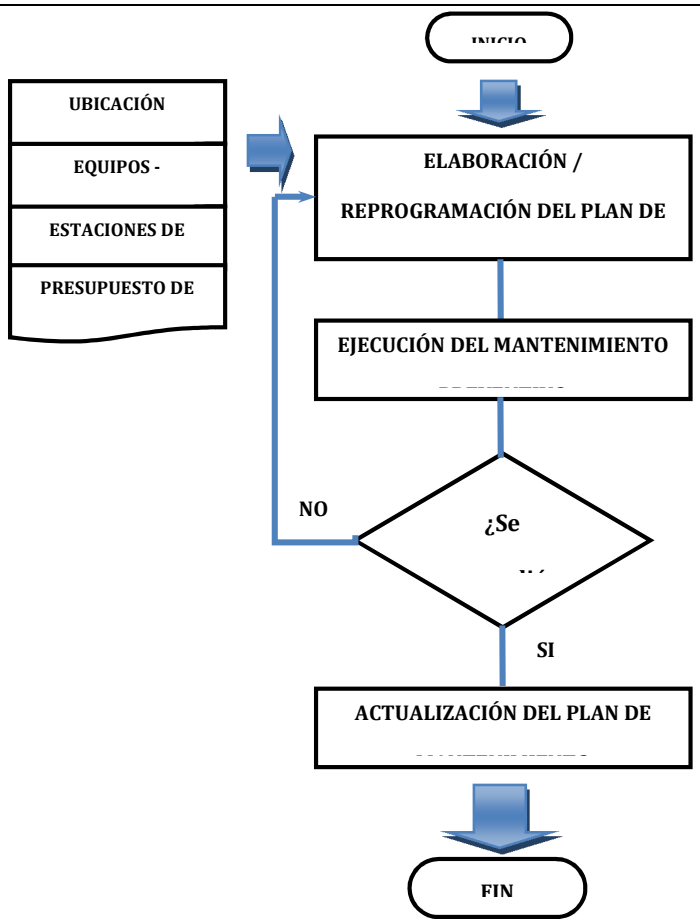
En el caso de las laptop se realizará únicamente mantenimiento del Software. Los mantenimientos correctivos de hardware se realizarán exclusivamente a las laptops que están fuera de garantía, aquellas que están bajo garantía y presenten problema de hardware serán remitidas al proveedor para evitar perder la garantía.

El mantenimiento de los servidores, routers, switch y UPS se lo realiza fuera del horario de trabajo de los usuarios del Grupo Agripac para no interrumpir las actividades de los usuarios. Se lo realizan preferentemente los fines de semana o feriados.

El mantenimiento en las estaciones de trabajo y demás periféricos que utilizan los usuarios, se lo realiza en horario laborable en coordinación con cada usuario.

5.1 Mantenimiento Preventivo.

MANTENIMIENTO PREVENTIVO		
Flujo de Proceso	**Responsable**	**Documento Asociado**



Gerente de Sistemas

Adiministrador de Sistemas

Personal de Soporte Técnico

Administrador de Seguridad

Administrador de Base de Datos

Gerente de Sistemas

5.2 Mantenimiento Preventivo Software.

El mantenimiento de software incluye: sistema operativo, antivirus, aplicativos, archivos de datos, parches y actualizaciones de cada uno de ellos.

Antivirus

Un antivirus es un programa que detecta virus en la computadora. Debido a que un virus es un programa o parte de un código que se carga en la computadora sin el consentimiento del usuario y se activa aunque el usuario no lo desee, el antivirus utilizado en Agripac está configurado para bloquear y eliminar Software maliciosos.

El antivirus se ejecuta cada vez que el usuario enciende la máquina para hacer su examen diario. Las unidades que analiza éste antivirus son: Discos Locales, Unidades Extraíbles, Unidades de CD y Archivos del Sistema. Durante el mantenimiento preventivo se realizara un scan completo de análisis de virus.

Desfragmentación:

La desfragmentación se realiza en cada mantenimiento y consiste en agrupar por tipo de archivo la información guardada en el disco.

Dependiendo del sistema de almacenamiento que utilice la computadora, esta podría estar cada vez más desordenada, con fragmentos del mismo archivo en diferentes partes del dispositivo. Para acceder a un archivo, la computadora tendría que buscar todos los fragmentos y combinarlos, lo cual afecta al rendimiento del computador. El proceso de desfragmentación organiza todos los segmentos de archivos, reduciendo el tiempo perdido buscando y combinando los diferentes segmentos. Además de mayor velocidad, se aumenta la vida del disco duro, ya que tiene que realizar menos movimientos.

Limpiar el disco duro

Todos los programas innecesarios y que no se utilizan del disco duro deben ser eliminados. Así como también se deben eliminar los archivos innecesarios, por ejemplo los archivos en la papelera de reciclaje, los archivos temporales, o el caché de las páginas web que no se utilizan, lo que se consigue es liberar espacio que el resto de programas podrán utilizar. Eso sí, la desinstalación se tiene que hacer correctamente, con la opción Agregar o Quitar programas del panel de control, y no solo borrando la carpeta.

El mantenimiento del Software se deja registrado en el formato FP.INF.004-02 Mantenimiento de Equipos.

Se aprovechará los mantenimientos para actualizar los drivers o parches que los diferentes software hayan publicado, especialmente aquellos que eliminan los huecos que permiten ataques de virus, programas maliciosos o aquellos

que puedan ser explotados por hackers para sustraer o alterar la información de la base de datos para cometer fraudes u otros delitos informáticos. Asimismo se verificará que no hayan sido alterada la seguridad del sistema operativo y que no se hayan instalados programas o software que no son utilizados ni autorizados por la empresa.

MEDIO AMBIENTE, SEGURIDAD Y SALUD EN EL TRABAJO

Ver control Operacional en la Matriz de Identificación de Peligros y/o Aspectos y Evaluación de Riesgos e Impactos.

PLAN DE CONTINGENCIA

NO APLICA

ANEXOS

NO APLICA

REGISTROS

CÓDIGO	NOMBRE	UBICACIÓN	TIEMPO DE RETENCIÓN	MEDIO	RESPONSABLE
FP.INF.004-01	Plan de Mantenimiento Preventivo	Mantenimiento	3 años	Físico / Electrónico	Gerente de Sistemas
FP.INF.004-02	Mantenimiento de Equipos	Mantenimiento Preventivo / Correctivo	Indefinido	Físico	Asistente de Gerencia

REGISTROS

CÓDIGO	NOMBRE	UBICACIÓN	TIEMPO DE RETENCIÓN	MEDIO	RESPONSABLE
FP.INF.002-01	Formulario S6:Solicitud de Servicios de Sistemas	Archivo de sistemas	4 años	Físico	Asistente de Gerencia de Sistemas
FP.INF.002-02	Formulario S1: Solicitud de Requerimiento	Archivo de sistemas	4 años	Físico	Asistente de Gerencia de Sistemas
FP.INF.002-03	Formulario S2: Análisis Técnico	Archivo de sistemas	4 años	Físico	Asistente de Gerencia de Sistemas
FP.INF.002-04	Formulario S3: Ficha Técnica de Modificaciones	Archivo de sistemas	4 años	Físico	Asistente de Gerencia de Sistemas
FP.INF.002-05	Formulario S4: Prueba de Requerimientos y Modificaciones	Archivo de sistemas	4 años	Físico	Asistente de Gerencia de Sistemas

INFRAESTRUCTURA TECNOLÓGICA, AMBIENTES Y PROCEDIMIENTOS DE LOS SISTEMAS DE INFORMACIÓN IT DE

AGRIPAC S. A.

Dpto. de Sistemas y Comunicaciones (TI)

2014
Actualizado a Abril-2014

Actualizaciones:

Marzo	**15**	**2007**
Octubre	**10**	**2008**
Noviembre	**14**	**2009**
Septiembre	**15**	**2010**
Febrero	**11**	**2011**
Mayo	**15**	**2012**
Abril	**01**	**2014**

Contenido Pág.

Agripac S. A. **Dpto. De Sistemas**

DESCRIPCIÓN DE LA INFRAESTRUCTURA TECNOLOGICA, DEFINICIÓN DE LOS AMBIENTES Y PROCEDIMIENTOS DE LOS SISTEMAS DE INFORMACIÓN IT DE AGRIPAC S. A.

INTRODUCCIÓN.

La eficiente instalación, distribución y funcionamiento de la Infraestructura tecnológicas IT y el eficiente uso de los recursos tecnológicos son vitales para el desarrollo de las actividades de la organización. La correcta definición de las funciones entre los ambientes de producción y desarrollo y la aplicación de procedimientos para la evaluación, adquisición y modificación de las aplicaciones de los sistemas de Información, permitirán proporcionar información segura, oportuna y efectiva bajo una relación de costo-beneficio que justifique que los sistemas instalados en hardware y software han sido la mejor opción para la empresa.

OBJETIVO.-

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.

ALCANCE.

El propósito de esta fase es dejar definido los diferentes ambientes de la infraestructura de los sistemas de información, el campo de acción así como el límite y responsabilidades de los administradores, analistas, programadores, soporte a usuarios y operadores quienes deberán realizar sus funciones en los ambientes definidos en este procedimiento, esto permitirá garantizar la seguridad, calidad, integridad y confiabilidad de la información.

INFRAESTRUCTURA DE SISTEMAS

Agripac cuenta con una completa infraestructura tecnológica que le permite cubrir todas las unidades (locales y remotas) de la organización, varias de esas unidades remotas están configuradas como segmentos de redes de cada una con un importante grupo de usuarios quienes están integrados a toda la organización a través de diversos tipos de enlaces como son: Fibra óptica, micro ondas, radios, etc., que les permite disponer en línea de los servicios de mensajería, acceso a la información, Internet, canales de voz, cámaras así como acceso directo a otros servicios de información.

La infraestructura tecnológica de Agripac está basada tecnología BLADE que agrupa hasta 16 servidores en un mismo chasis, actualmente tiene incorporado cuatro para el manejo de la base de datos y el Sistema de Información ERP-SAP (desarrollo, calidad, producción y backup), detalles en el Anexo A, tres para los servicios de mensajería, seguridad de la red, comunicación y dispositivos móviles.

La infraestructura de servidores para el sistema de información es de tecnología Blade cuyos servidores (desarrollo, producción, calidad y backup), son servidores Intel, el sistema operativo es el LINUX RED HAT, sobre los cuales está instalado un motor de Base de Datos Oracle, el sistema de información es el ERP-SAP, cuyos módulos cubren todas las áreas de la organización.

Los dos servidores para administrar la mensajería y la seguridad de la red trabajan bajo la plataforma de productos Microsoft, como son Windows Server 2008, Exchange 2008, Microsoft Mail y un Firewall Isa Server para control de la seguridad cumpliendo la función de Firewall, el control de virus y restricciones de mensajería y navegación es complementada a través de una suite de software Mail Scan para servidor, detalles adjunto en anexo C.

Los diferentes ambientes están definidos de la siguiente forma:

AMBIENTE DE DESARROLLO.

El ambiente de desarrollo está soportado por un servidor Linux al que tienen acceso los analistas programadores así como los consultores y Basis SAP para realizar nueva programación, cambios en la configuración de los módulos de SAP y pruebas de programas previo a su paso a producción, a este servidor cada cierto tiempo se transfiere la base de datos desde el Servidor de Producción con la finalidad de mantener actualizados los cambios realizados en la base de datos, el responsable de la administración de la base de datos y de los códigos fuentes transfiere el o los códigos que requieren ser modificados, para que los analistas programadores realicen la programación y pruebas de las tareas asignadas, una vez concluidos en conjunto con el responsable de la calidad de la información y el usuario realizan las pruebas correspondientes, si ésta se ajusta a lo solicitado que consta en los respectivos formularios funcionales, el responsable de administrar el servidor de producción una vez que recibe la autorización del gerente de sistemas, procede a transferir el código al servidor de producción donde es revisado y posteriormente compilado para que empiece a funcionar.

AMBIENTE DE PRODUCCION

El ambiente de producción está bajo la responsabilidad del Administrador de la Base de Datos BASIS-SAP quien es el encargado de administrar la base

de datos y el sistema operativo. Los accesos así como la administración de roles y Perfile está a cargo del administrador de Seguridad quien además se encarga de crear los transportes de los códigos fuentes de SAP para que los programadores realicen las modificaciones y cambios en los códigos “Z”. El procedimiento para realizar una modificación a uno o varios códigos o para desarrollar un código nuevo es el siguiente.

Una vez que el requerimiento del usuario es analizado en conjunto entre el gerente y subgerente de sistemas y cuando es necesario con la participación del administrador, los funcionales de SAP y los analistas programadores (dependiendo del módulo), después de ser aprobado por la gerencia de sistemas, el oficial de Seguridad procede a transferir el o los códigos fuentes al servidor de desarrollo para que el programador a quien se le asignó el caso pueda realizar el desarrollo del requerimiento y una vez que han concluido con el mismo comunica al sub-gerente quien en conjunto con el usuario verifican y realizan las pruebas necesarias para determinar que cumplen con lo solicitado si hay alguna inconformidad se comunica al analista programador para que realice el corrección, si está conforme se comunica su cumplimiento al gerente de sistemas quien autoriza al oficial de roles y perfiles para que el requerimiento sea transferido a producción dejando constancia de ello en el respectivo formulario.

AMBIENTE DE BACKUP-REPLICACION EN LÍNEA.

La seguridad física y lógica de la información es vital para que la organización pueda reaccionar ante cualquier contingencia para ello se cuenta con un servidor de replicación o backup que tiene características de procesamiento y almacenamiento similares al servidor de producción, este servidor está ubicado en las instalaciones de una de las empresas del grupo (Balanfarina) cuyas instalaciones se encuentran en el 6.5 Km de la vía Durán Tambo, este servidor está conectado al servidor de producción mediante un enlace micro onda de 5 MB.

La actualización de la base de datos desde el servidor de producción al servidor de replicación backup se realiza en línea mediante la herramienta de Replicación de datos desarrollado sobre la base de datos ORACE, que transmite las páginas actualizadas cada 5 minutos, este proceso de respaldo redundante garantiza a la organización contar con un respaldo en línea que le permitirá reaccionar de manera inmediata ante cualquier contingencia.

Los tres ambientes mencionados deben ser respaldados para garantizar que la información almacenada en estos equipos pueda ser recuperada ante la eventualidad de un siniestro o cualquier contingencia. Más adelante describiremos los procedimientos de respaldo que tenemos en el ambiente de desarrollo, ambiente de backup y de producción.

El procedimiento de respaldo en cintas magnéticas fue reemplazado por unidades de discos externos que resultan más eficientes y fácil para recuperar cualquier archivo, los respaldos son sacados diariamente sobre el un disco que forma parte del Storage de almacenamiento, además semanalmente es almacenado en el casillero de seguridad del Banco Bolivariano, este es otro tipo de respaldo que garantiza la recuperación del activo más valioso de la organización como es la información. Las frecuencias de los diferentes respaldos a sacarse son:

En línea (Réplica), Diario, Semanal, Mensual

Con la finalidad de asegurarse el cumplimiento de este proceso, se tiene el siguiente proceso establecido.

La persona responsable de sacar diariamente el respaldo, registra en la bitácora los siguientes datos:

Fecha del respaldo

Hora del Respaldo

Servidor

Tipo de Respaldo

Contenido

Ubicación física

Operador

Firma

Esos mismos datos son registrados en la etiqueta del SDLT y trasladados al casillero de seguridad de la bóveda del Banco Bolivariano por una las tres personas autorizadas y registradas en el contrato con el Banco que son: Ing. Roberto Cayetano, Sr. Carlos Suárez y/o Ing. Bolívar Vallejo.

Este procedimiento es conocido por todos los participantes en cada una de los ambientes mencionados, siendo responsabilidad de cada uno de ellos en cumplir las disposiciones impartidas en este procedimiento.

El gerente de sistemas tiene la responsabilidad de monitorear periódicamente para que se cumplan estas disposiciones y hacer las recomendaciones y modificaciones a este procedimiento para mantenerlo actualizado de acuerdo a los cambios que se hicieren necesario.

Agripac S. A. **Dpto. De Sistemas**

POLÍTICAS Y PROCEDIMIENTO PARA LA ADQUISICIÓN, IMPLEMENTACIÓN, DESARROLLO Y MANTENIMIENTO DE LAS APLICACIONES

OBJETIVO

Proporcionar soluciones de tecnología IT, en hardware y software que están alineadas con los objetivos del negocio.

Proporcionar las plataformas apropiadas para soportar aplicaciones de negocios.

ALCANCE

La adquisición de hardware y software deberán seguir las políticas de adquisición de la organización.

La Gerencia deberá desarrollar e implementar políticas y procedimientos que permitan asegurar la selección de los mejores proveedores y que garanticen la selección de software de acuerdo a las necesidades del negocio así como la compatibilidad y estandarización de la plataforma de la organización.

GENERALIDADES

Deberán establecerse procedimientos para evaluar la compatibilidad y el impacto del nuevo software sobre el rendimiento de la aplicación central.

La Gerencia de sistemas de información deberá asegurar que la instalación del nuevo software no ponga en riesgo la seguridad de los datos y demás programas del sistema de información. Deberá dar mucha importancia a la instalación y mantenimiento de los parámetros del nuevo software.

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, los que deben estar alineados con los objetivos de la organización, 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. Los proveedores deben ser calificados tomándose en cuenta los siguientes requisitos mínimos.

    a. El proveedor debe tener representante en el país, mínimo un año.
    b. EL proveedor debe haber sido calificado y cumplir con los requisitos especificados por el Sistema de Gestión de Cambios.
    c. Mínimo se debe analizar tres ofertas bajo las condiciones y características similares.

2. Se deben analizar varias soluciones de proveedores calificados cuyos productos cumpla con las exigencias de calidad mínimas establecidas.

3. 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 auditoría, 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.

4. Considerando que la empresa requiere tener autonomía en el manejo de sus aplicaciones por ello cuenta con su propio equipo de sistemas, se recomienda en lo posible 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, previamente con su personal determinan la necesidad de información para su gestión, ésta es planteada a la gerencia general quien lo canaliza a través del Comité que está conformado por el gerente general, gerente de operaciones, gerente financiero, gerente de sistemas y gerente de SGI, dicho Comité analiza el requerimiento, especialmente el objetivo, alcance y que dicho requerimiento esté alineado con los objetivos de la organización, se determinan, recursos y tiempos para en base a ello determinar su aprobación.

La gerencia de sistemas en conjunto con su equipo analizará los requerimientos técnicos de hardware y software y determinan la factibilidad de desarrollarlo In-House o recomendar la adquisición de una solución que exista en el mercado para ese objetivo.

Todo desarrollo “Z” que se realice In-House debe sujetarse al standard establecido por SAP, la integración no debe impactar los tiempos de respuesta del ERP ni alterar la configuración de ningún módulo del ERP.

Cualquier aplicativo o módulo que se desee adquirir debe estar certificado para trabajar con SAP.

En caso que la recomendación sea desarrollarlo con el equipo propio, se determinan 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 de 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 por SAP, además de cumplir con todo lo recomendado en los procedimientos establecidos en la organización.

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 formulario 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 estándar 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.

FORMULARIO PARA REGISTRAR SOLICITUDES DE PROGRAMAS NUEVOS O MODIFICACIONES

Objetivo.-

La principal función de los formularios es llevar un control de lo solicitado por parte del usuario, la asignación del analista programador, las tareas que se deben desarrollar, el tiempo que tardará la ejecución de esta solicitud, y documentará todas las etapas que se desarrollan para implementar los nuevos programas o las modificaciones.

Formulario: FP.INF.002-02 Descripción: SOLICITUD DE REQUERIMIENTO

INSTRUCTIVO

El formulario FP. INF. 002-02 es el documento que utilizarán los usuarios de sistemas para requerir del área, 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 solicitante

USUARIO: Nombre del solicitante, Gerente o Jefe de área

FECHA: Fecha de la solicitud

Los casilleros ubicados en la parte superior derecha del formulario deberán llenarse con la siguiente información:

REQUERIMIENTO: Marcar este casillero en caso de solicitar una nueva

FORMULARIO PARA ANALISIS TECNICO

Objetivo

El principal objetivo de este formulario, es un informe del análisis técnico llevado a cabo por el analista programador asignado, en donde hace una descripción de cómo realizara los cambios a los códigos necesarios.

Formulario: FP.INF.002-03 Descripción: ANALISIS TECNICO

Instructivo

GERENTE DE SISTEMAS Pie de firma del gerente del área.

FORMULARIO FICHA TECNICA DE MODIFICACIONES

Objetivo

Este documento interno permitirá llevar un control del desarrollo de los nuevos requerimientos, y de 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 deben ser modificados, y la fecha de entrega del proyecto.

Formulario: FP.INF.002-04 Descripción:

FICHA TECNICA DE MODIFICACIONES

Instructivo

FP.INF.002-04	Número consecutivo único que debe tener relación con los demás formularios utilizados para esta modificación.
FECHA:	Fecha de asignación del analista al proyecto.
COMPAÑÍA	Nombre de la empresa.
PROCESO:	Nombre del proceso afectado.
MODULO:	Nombre del módulo al que corresponde el requerimiento.

PRIORIDAD:	Requerimos del usuario determinar con una letra en este casillero la prioridad que se debe aplicar a este requerimiento. B=baja, M=media, A=alta.
RESPONSABLE PROYECTO	Nombre del analista a cargo del proyecto.
FECHA MAXIMA ENTREGA	La fecha en la que se entregará el proyecto.
CUMPLIMIENTO:	Fecha en la que se cumplió el proyecto.
CODIGO:	Nombre del programa fuente que debe ser modificado.
DETALLE MODIFICACION:	Se describe el cambio que se hará al código fuente.
ANALISTA RESPONSABLE	Se registra el nombre o nombres de analista asignado al proyecto, se dan casos en los cuales hay varios analistas asignados a los proyectos.
TIEMPO ESTIMADO HORAS	Se registra el tiempo en horas que se estime necesario para realizar los cambios o modificaciones, al código. Para poder llevar un control de las tareas asignadas a cada programador.
FECHA ENTREGA ESTIMADA	Fecha tentativa de terminación de cambio en el Código.

FECHA ENTREGA REAL	Se registra a fecha en la cual el analista termina de realizar los cambios.
CUMPLIMIENTO:	En este casillero se registra el cumplimiento comparando las 2 fechas, de entrega estimada y entrega real.
OBSERVACIONES:	En este punto se registran datos relativos al proyecto y que son relevantes.
ANALISTA RESPONSABLE	Pie de firma del analista responsable del proyecto.
GERENTE DE SISTEMAS	Pie de firma del gerente del área.

FORMULARIO PRUEBA DE REQUERIMIENTOS Y MODIFICACIONES

Objetivo

El formulario S4, es un instrumento interno que permite registrar las pruebas en el ambiente de desarrollo, y cuando estas han concluido, poder hacerlas con la participación del usuarios solicitante, una vez que el usuario solicitante acepta que el desarrollo o la modificación cumple con las expectativas o sus necesidades, procede a formar el respectivo formulario y se procede al último paso que consiste en pasar dicho cambio de desarrollo a producción por parte del responsable de esa función, quien una vez concluido ese paso procede a firmar dicho formulario para cerrar el caso.

El formulario es registrado por la asistente de sistema en el aplicativo que permite llevar dicho control, luego se archiva el formulario en la carpeta correspondiente.

Describiremos una serie de procedimientos y políticas que han sido necesarias adoptarlas para poder resguardar y precautelar la información, los servidores, los equipos de comunicaciones, y todos los procesos que desde esta área se generan, para garantizar el menor impacto posible ante la eventualidad de siniestros, sean estos accidentales, naturales o provocados.

SEGURIDADES FISICAS

El área de sistemas se encuentra ubicada en el último piso del edificio administrativo, para acceder a sistemas, se debe pasar por el control de los guardias de seguridad, por la recepción, siendo este recorrido grabado en cámaras de video.

Para ingresar a las oficinas de sistemas, la puerta cuenta con una cerradura eléctrica, que puede ser accionada desde adentro, o con la llave cuyos duplicados solo lo tienen quienes tienen autorización, el acceso está restringido a personas ajenas a la empresa, si alguien ingresa a sistemas debe haber recibido previamente la autorización del personal que labora en esta área. El acceso puede ser hasta la oficina del personal que autorizo dicho ingreso. No puede haber personas ajenas a esta área que no estén plenamente identificadas ni pueden recorrer el área sin la supervisión del personal de sistemas. Esto aplica a personal de la empresa que labora en otras áreas.

Alarmas

Se implementaron en toda el área sensores de movimiento, detectores de humo, que están siendo monitoreadas por la compañía que nos presta el servicio de seguridad. Además, estos sensores son activados con clave por la última persona en salir del área, y desactivados por el primero en llegar. Para

poder activar y desactivar las alarmas, todo funcionario tiene una clave secreta única, que lo identifica cuando hace uso de la misma. Las activaciones son monitoreadas desde la compañía de seguridad, llamando a la persona que desactiva la alarma, para verificar que no existan novedades.

Extintores

En el área están ubicados aparatos contra incendio, adecuado al tipo de equipos electrónicos.

PUERTA DE ACCESO A LA SALA DE SERVIDORES

En el centro de cómputo, se encuentran los diferentes servidores, entre ellos de producción, de desarrollo, de correo, de servicio de Internet, etc., además, la central telefónica y los equipos de comunicaciones para los enlaces con agencias y sucursales, al cual es restringido el acceso incluso para el personal de sistemas. Las personas autorizadas son el administrador de la red, y el administrador de la base de datos. Para el control de los accesos, hay una bitácora en donde se registra datos de las personas que por razones técnicas deben ingresar a dicha área.

Esta puerta debe permanecer cerrada, para evitar que ingrese alguien no autorizado.

En lo que respecta a las seguridades lógicas, a continuación describiremos una serie de procedimientos que nos permite precautelar la información y la funcionalidad de los equipos que están en el centro de cómputo.

Casillero de seguridad.

La empresa por gestión del gerente de sistemas, contrató un casillero de seguridad en la matriz del banco Bolivariano, con la finalidad de guardar el activo más valioso de la empresa, la información.

En este casillero, se guardan diariamente, los discos de respaldos de los servidores de producción y de desarrollo, los respaldos en CD y DVD de los programas fuentes tanto del sistema puntos de venta, como de los programas desarrollados en Visual, y sistemas como el de recursos humanos, control de mantenimiento de vehículos, etc.

Llevando una bitácora el registro de los respaldos diarios de los servidores de producción y desarrollo.

Centro de cómputo alterno

Con la finalidad de estar preparados en casos de siniestros, está en fase de implementación un centro de cómputo alterno, para mantener un respaldo en línea del servidor de producción, y del servidor de correo electrónico, que están ubicados en la planta de Balanfarina.

Estos servidores estarán permanentemente actualizados, con el objetivo de seguir brindado el mismo servicio que los servidores de producción y de correo.

El servidor de producción de SAP (incluye Base de Datos, Configuración y Códigos Fuentes), se actualiza en línea mediante un esquema de replicación desarrollado para Oracle, que permite que la base definida como primaria instalada en el servidor de producción (Agripac), actualice cada 10 minutos la base del servidor de respaldo (Agripac2) mediante un proceso de replicación. Como podemos apreciar, en casos de contingencias que afecte total o parcialmente el servidor de producción la empresa podrá retomar sus operaciones en un lapso de tiempo muy corto porque tenemos otro servidor de producción con la información hasta 10 minutos antes del siniestro.

SEGURIDAD EN PROVISION 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 alterno 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 de baja el breaker master y luego se apaga el generador.

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.

HERRAMIENTAS O DISPOSITIVOS DE SEGURIDAD DE INFORMACIÓN UTILIZADA.

Siendo la información el activo más valioso para la organización, es de vital importancia su protección y uso adecuado de la misma, el acceso que tienen los usuarios debe ser estrictamente a la información necesaria para realizar sus labores, siendo de su única responsabilidad por el mal uso que se haga de la misma.

Para ello se han determinado roles y perfiles de acuerdo al requerimiento de cada cargo de tal manera que de acuerdo al cargo del usuario se le asigna el rol que le corresponda, esta es una buena práctica que forma parte de la metodología de SAP, la misma que ha sido incorporada en nuestros procedimientos, además a cada usuario se le asigna un login y un password para ingresar al sistema el mismo que está atado al rol del usuario y de acuerdo al rol el sistema le asigna el menú, las claves se deben cambiar mínimo tres veces al año.

El acceso a la información se realiza a través de un menú que permite el acceso solo a la información autorizada para un determinado usuario.

Ciertos programas considerados críticos tienen una clave adicional en el código la misma que es conocida solamente por la persona autorizada, además el sistema lleva un archivo de auditoria donde se registran todas las

modificaciones, reflejando el contenido anterior y el actual del campo modificado, la fecha y hora de modificación, sí como el operador que lo hizo.

El acceso al servidor de producción donde reside la base de datos se lo realiza a través del servidor de mensajería el mismo que está protegido con el software de seguridad UTM Cyber roam (manejo integrado de amenazas) que cumple la función de Proxi y de Firewall, el mismo que está configurado para no permitir el ingreso de intrusos desde el exterior así como el ingreso a la red de personas no autorizadas, ya que maneja perfiles de usuarios individual y por grupos.

POLÍTICAS DE SEGURIDAD DE INFORMACIÓN

Las políticas de seguridad establecidas son:

1. El acceso a la información se lo realiza a través de claves que solo la conocen las personas autorizadas.
2. Cualquier requerimiento de información es previamente analizado y autorizado por la gerencia general.
3. No se permite el ingreso a la sala de máquina de personas no autorizadas.
4. El acceso al departamento de sistemas se restringe solo para personal autorizado.
5. Las claves de seguridad asignada a cada usuario no deben ser divulgadas a ninguna otra persona ni prestada por ningún motivo.
6. La clave del administrador y de acceso a la base de datos es manejada solo por el gerente de sistemas y el administrador de la base de datos.
7. Los cambios o modificaciones se deben realizar en el servidor de desarrollo, bajo ninguna circunstancia se debe realizar en el servidor de producción.
8. Los códigos fuentes deben estar protegidos bajo una clave de tal manera que los programadores solo puedan acceder al programa fuente desbloqueado para realizar mantenimiento o modificación autorizada.

A continuación explicaremos los procedimientos de respaldos que aplican a los servidores de cada ambiente:

PROCEDIMIENTO DE ADMINISTRACION DE PROGRAMAS FUENTES

SISTEMA: SAP

Objetivos

Proveer de manera documentada los procedimientos que permitan administrar los códigos fuentes de la aplicación SAP, el control de los cambios que se efectúen, las pruebas, que interpreten lo solicitado por los usuarios, cumpliendo de esta manera las normas de seguridad y los estándares que en estos casos se requiere.

Establecer seguridad en el uso adecuado de los programas fuentes y los objetos que están en producción, controlando que el proceso de cambios y pruebas cumplan con los estándares y cumpliendo estrictamente la finalidad de tener una aplicación segura disminuyendo la posibilidad de accesos no deseados, para lo cual se deberá seguir los siguientes pasos:

Procedimiento

1. El usuario debe llenar el formulario FP.INF.002-02, en donde se hace el requerimiento a Sistemas.

2. El Gerente de Sistemas evalúa y asigna el requerimiento a algún analista programador.

3. El analista establece el alcance de los cambios y solicita al administrador del sistema de producción los fuentes que requiera, para el efecto utiliza el formulario FP.INF.002-03 “Análisis técnico” en donde registra el detalle de los programas. En aquellos casos en los cuales el usuario no lleno el formulario FP.INF.002-02, es responsabilidad del técnico asignado hacerlo, y recoger la firma del usuario.

4. El administrador pasa los códigos fuentes solicitados al ambiente de desarrollo, en el directorio que corresponda, e informa al analista.

5. El administrador guarda una copia de la versión del programa requerido, para que una vez cambiado, tengamos una copia de estos programas antes de ser modificados.

6. Cuando el analista asignado al caso indique que la modificación está concluida, debe hacer las pruebas necesarias en el ambiente de desarrollo junto con el administrador de producción, haciendo notar que están cumplidos los cambios solicitados.

7. El analista devuelve los códigos fuentes al administrador para que este los ponga en producción.
8. El administrador deberá revisar el fuente para determinar que los cambios efectuados cubren los requerimientos solicitados por el usuario en el formulario.
9. Revisados los cambios, el administrador compila los programas y los ubica para que estén disponibles en el ambiente de producción. En caso de no haber novedades, seguir con el paso 12 de este instructivo.
10. En caso de presentarse problemas, debe revisar de manera inmediata junto con el analista asignado al caso, lo que debe corregir, dejando sin efecto el cambio hasta que estén seguros que los cambios da los resultados esperados.
11. Luego de la revisión y corrección del fuente, se debe volver al punto 6 de este instructivo.
12. El administrador debe confirmar que los fuentes y objetos queden ubicados en los directorios correspondientes de acuerdo a la estructura que tiene la aplicación de Elite.
13. El administrador debe proceder a respaldar la aplicación con los últimos cambios.

PROCEDIMIENTO DE ADMINISTRACION DE PROGRAMAS FUENTES

PROGRAMAS: VISUAL

Objetivo

Administrar apropiadamente los códigos de los programas desarrollados en Visual 6, los mismos que cumplen un factor importante dentro de la empresa ya que llevan procesos como Nóminas, contabilidad, etc., de todas las empresas relacionadas, y deben ser controlados los cambios que se realizan.

Los cambios de los programas deben ser debidamente soportados por documentos en donde los usuarios que los utilizan deben requerir los cambios pertinentes, y estos deben ser aprobados por la gerencia de sistemas antes de ser modificados, y luego ser puestos en producción.

Para esto hemos elaborado el siguiente procedimiento:

1. El usuario debe llenar el formulario FP.INF.002-02, en donde se hace el requerimiento a Sistemas.
2. El Gerente de Sistemas evalúa y asigna el requerimiento a algún analista programador.
3. El analista establece el alcance de los cambios y solicita al administrador del sistema de producción los fuentes que requiera, para el efecto utiliza

el formulario FP.INF.002-03 “Análisis técnico” en donde registra el detalle de los programas. En aquellos casos en los cuales el usuario no lleno el formulario FP.INF.002-02, es responsabilidad del técnico asignado hacerlo, y recoger la firma del usuario.

4. El administrador pasa los fuentes o librerías solicitados al ambiente de desarrollo, en el directorio que corresponda, e informa al analista. En estos casos, el ambiente de desarrollo es en la estación de trabajo del analista programador.

5. El administrador guarda una copia de la versión del programa requerido, para que una vez cambiado, tengamos una copia de estos programas antes de ser modificados.

6. Cuando el analista asignado al caso indique que la modificación está concluida, debe hacer las pruebas necesarias en el ambiente de desarrollo junto con el administrador de producción, haciendo notar que están cumplidos los cambios solicitados.

7. El analista devuelve los fuentes al administrador para que este los ponga en producción.

8. El administrador deberá revisar el código fuente para determinar que los cambios efectuados cubren los requerimientos solicitados por el usuario en el formulario.

9. Revisados los cambios, el administrador compila los programas y los ubica para que estén disponibles en el ambiente de producción. En caso de no haber novedades, seguir con el paso 12 de este instructivo.

10. En caso de presentarse problemas, debe revisar de manera inmediata junto con el analista asignado al caso, lo que debe corregir, dejando sin efecto el cambio hasta que estén seguros que los cambios da los resultados esperados.

11. Luego de la revisión y corrección del fuente, se debe volver al punto 6 de este instructivo.

12. El administrador debe confirmar que los fuentes y objetos queden ubicados en los directorios o estaciones de trabajo correspondientes.

13. El administrador debe proceder a respaldar la aplicación con los últimos cambios.

Procedimiento de respaldos de servidor de producción

En el servidor de producción debemos respaldar la base de datos, los directorios de usuarios y del sistema operativo.

- **Procedimiento de respaldo de la base de datos**

  Objetivo

  La base de datos debe ser respaldada diariamente, para el efecto hay un proceso que se ejecuta automáticamente, el mismo que hay que revisar diariamente en el archivo "/f/oracle/ontape.log" para revisar los mensajes de ejecución del respaldo, ya que se ejecuta cuando termina de hacer el proceso "update statistics", aproximadamente a las 5:20 am.

  Frecuencia: Diario/semanal/mensual

  Responsable: Administrador de base de datos y seguridades

  Formato de respaldo: comando dd (ontape)

  Procedimiento

  1. Tener la precaución de poner diariamente el disco externo que corresponde para el respaldo

2. Ingresar como usuario “Oracle”
3. Revisar el archivo “/f/Oracle/ontape.log” en donde muestra la hora de inicio y de terminación del respaldo.
4. Si el proceso muestra que a realizado el proceso automáticamente, sacar la cinta y etiquetarla con la fecha y hora del respaldo.
5. En caso de no haber ejecutado el proceso, hacerlo manualmente con el siguiente comando: $ ontape –s –L 0
6. Luego sacar y etiquetar la cinta.
7. Llevar la cinta al casillero de seguridad del banco.
8. En el casillero, poner la cinta del día, y retirar la cinta que tenga etiquetada la fecha del día que corresponde, y que son reutilizadas diariamente de lunes a viernes.
9. Llenar el bitácora registrando la información respaldada.

El servicio de casilleros del banco Bolivariano atiende de lunes a viernes de 8:30 am a 16:30 pm. Y debe escoger un turno indicando que desea ir a casilleros y en atención de servicios bancarios cuando le toque el turno lo llevarán para guardar el respaldo, previa presentación de cédula de identidad.. Para el respaldo mensual requerimos 12 cintas, siendo estas reutilizadas, y 7 cintas para respaldar diariamente.

Procedimiento de respaldo de usuarios y aplicación

Objetivo.

En este respaldo se copian los directorios (filesystems) /c /cooperativa /d /e /f /prg /u con lo cual tenemos todos los archivos y perfiles que pertenecen a cada usuario, el software de la base de datos “Oracle”, con todas sus configuraciones, la aplicación con sus programas fuentes, objetos, librerías y procedimientos.

Frecuencia:	Mensual
Responsable:	Administrador de base de datos y seguridades
Formato de respaldo:	comando tar

Procedimiento

1. Poner la cinta en la unidad respectiva.
2. Ingresar al sistema como usuario “root”.
3. Ejecutar el comando: tar –cv8 /c /cooperativa /d /e /f /prg /u
4. Una vez terminado el respaldo, etiquetar la cinta correspondiente.
5. Llevar la cinta al casillero de seguridad del banco.
6. Retirar la cinta etiquetada con el nombre del mes que sigue.

7. Llenar la bitácora registrando el respaldo efectuado.

Este proceso requerirá de 12 cintas, las mismas que se reutilizaran cuando el mes que se desea respaldar coincida con la etiqueta que tiene la cinta.

Procedimiento de respaldos de servidor de desarrollo

Objetivo.

En el servidor de desarrollo es importante mencionar que la base de datos no es actualizada con las transacciones diarias que generan los movimientos comerciales de la empresa, sino que es una copia de la base de producción, por lo que no es necesario respaldar esta base de datos. Sin embargo describiremos el procedimiento bajo el cual restauramos la base, para que el ambiente de pruebas tenga lo más actualizado posible la base. Pero si es de mucha importancia respaldar los directorios de usuarios y de la aplicación, y del sistema operativo.

Procedimiento de respaldos de servidor de replicación

Objetivo.

En el servidor de replicación es importante mencionar que la base de datos no es actualizada con las transacciones diarias que generan los movimientos comerciales de la empresa, sino por medio de un proceso de replicación configurado en el motor de la base de datos, en donde la base del servidor de producción es definida como primaria, cada 30 segundos actualiza la base del servidor definido como secundario, con lo cual podemos tener un respaldo actualizado en caso de algún percance.

Podemos concluir que el servidor de replicación es sin duda una copia del servidor de producción, ya que el propósito de este equipo es que en caso de contingencia, este se convierta en el servidor de producción. Por ello debe estar los más actualizado posible.

Procedimiento de restauración de la replicación de la base de datos

Objetivo.

El proceso de replicación actualiza de una base definida como primaria a otra base definida como secundaria, a la cual pasa las últimas páginas que hayan sido modificadas durante los últimos 30 segundos.

Es necesario mencionar lo importante de este proceso, ya que nos permite hacer pruebas de recuperación desde las cintas, con lo cual verificamos que los respaldos están correctos.

Frecuencia: Cuando se corte la replica

Responsable: Administrador de base de datos y seguridades

Formato de restauración: Comando dd (ontape)

Este proceso requiere que ningún usuario ingrese al sistema, por lo cual debe ser hecho en horas no laborables.

Procedimiento

1. Ingresar como usuario “Oracle” tanto en el servidor de producción como de replicación.
2. Bajar el motor de la base de datos del servidor de replicación, con el comando: “ $ ontape –ky”
3. En el servidor de producción hacer el respaldo de la base a nivel 0, con el comando: “ $ ontape –s –L 0”
4. Ejecutar en el servidor de producción el comando “ $ onmode –d primary agripac2”
5. En el servidor de replicación una ves terminado el respaldo, ejecutar el comando “$ ontape –p” con lo cual restauramos la base de datos.
6. A las preguntas que hace el proceso de restauración contestar “n”.
7. Una vez terminado el proceso de bajar el respaldo de la base, ejecutar el comando “onmode –d secondary agripac”, en el servidor de replicación.
8. Con este comando las bases de datos de ambos servidores se sincronizan y cuando lo logran se actualizan automáticamente cada 30 segundos.
9. La base del servidor definido como secundario se levanta en modalidad solo de lectura, lo cual garantiza que el servidor secundario solo pueda ser actualizado mediante el proceso de réplica.

10. Para verificar que está levantada la replicación puede ejecutar el comando “$ onstat –g dri” , esto le indicará el estatus de “on” a la replicación.
11. Registrar en el bitácora el ingreso y egreso del centro de cómputo alterno, indicando la actividad desarrollada.

Procedimiento de restauración de usuarios y aplicación

Objetivo.

El respaldo emitido en el servidor de producción debe servir para actualizar los filesystem o directorios de usuarios y de aplicaciones del servidor de replicación, ya que este debe estar lo más actualizado posible en caso le toque ser convertido en el servidor de producción.

Frecuencia:	Semanal
Responsable:	Administrador de base de datos y seguridades
Formato de respaldo:	comando tar

Hay que bajar íntegramente el respaldo, para garantizar que actualiza todo.

Procedimiento

1. Poner la cinta en la unidad respectiva.
2. Ingresar al sistema como usuario “root”.
3. Ejecutar el comando: tar –xv8 /c /cooperativa /d /e /f /prg /u
4. Una vez terminado la restauración, llevar la cinta al casillero de seguridad

Este proceso requerirá de 12 cintas, las mismas que se reutilizaran cuando el mes que se desea respaldar coincida con la etiqueta que tiene la cinta.

Procedimiento de respaldo del sistema operativo

Objetivo.

Con el administrador del sistema operativo “Rethat”, es posible hacer un backup del “filesystem” root, en donde está instalado el sistema operativo, el cual es necesario respaldarlo, ya que sería de mucha utilidad restaurarlo luego de presentarse alguna contingencia.

De esta manera se recuperan todas las configuraciones de dispositivos como impresoras, parámetros del kernel, etc. Este respaldo debe ser hecho cada mes, o cada que se cambie la configuración del sistema operativo.

Frecuencia: Mensual, o en cada modificación del kernel

Responsable: Administrador de base de datos y seguridades

Formato de respaldo: comando cpio

Procedimiento

1. Ingresar al sistema como usuario “root”
2. Ingresar la cinta en la unidad de respaldo
3. Ejecutar “scoadmin”

4. Escoger la opción de backup manager, backup, run unscheduled, select filesystem.
5. Seleccionar el filesystem “/dev/root”
6. Escoger el dispositivo de respaldo y la capacidad de la cinta
7. Una vez terminado el proceso, etiquetar la cinta
8. Llevar la cinta al casillero de seguridad del banco.
9. Registrar en la bitácora el respaldo.

Procedimiento de respaldo de servidor de correo

Frecuencia: Semanal

Responsable: Administrador de red

Formato: Imagen de disco

Procedimiento de respaldo de aplicaciones visual

Objetivo.

Los programas realizados utilizando el front end Visual 6, tenemos varios módulos que prestan servicio a las compañías filiales como Agrigrain, en donde se lleva un control de inventarios de granos, el sistema de nominas de todas las empresas, tenemos el sistema de contabilidad de Celtec, Skiper y Agrigrain, el módulo de control de mantenimiento de vehículos y el control de inventario del taller. Además, se cuenta con el módulo de autorizaciones de crédito, el módulo de control de documentos de requerimientos a sistemas, módulo de control de cheques para autorizaciones de pagos en los bancos, módulo de control de entrada y salida de equipos partes y piezas de computadores, y el módulo de estadísticas.

Todos estos módulos están instalados en su ambiente de producción en un servidor con Windows XP, una copia de todos los códigos y librerías está en el servidor de desarrollo (agripac1), en donde es respaldado siguiendo el siguiente procedimiento:

Frecuencia: Diario

Responsable: Administrador de base de datos y seguridades

Formato: tar

Procedimiento

1. Poner la cinta en la unidad respectiva.
2. Ingresar al sistema como usuario “root”.
3. Ejecutar el comando: tar –cv8 /u/visual
4. Una vez terminado el respaldo, etiquetar la cinta correspondiente.
5. Llevar la cinta al casillero de seguridad del banco.
6. Retirar la cinta etiquetada con el contenido.
7. Llenar la bitácora registrando el respaldo efectuado.