

PRACTICA EMPRESARIAL PARA OBTENER EL TITULO

DE

INGENIERO DE SISTEMAS

MARTHA GLADYS SANCHEZ VASQUEZ

RUBEN DARIO MARULANDA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
FACULTAD DE CIENCIAS BASICAS E INGENIERIA
PROYECTO DE GRADO
PLAN DE CONTINUIDAD DE TECNOLOGÍA INFORMÁTICA
AREA ADMINISTRATIVA
BOGOTA, D.C., 2004**

**TESIS DE GRADO PARA OPTAR AL TÍTULO DE
INGENIERO DE SISTEMAS**

Directora

NANCY ESPINEL BERNAL

Ingeniera de Sistemas

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
FACULTAD DE CIENCIAS BASICAS E INGENIERIA
PROYECTO DE GRADO
PLAN DE CONTINUIDAD DE TECNOLOGÍA INFORMÁTICA
AREA ADMINISTRATIVA
BOGOTA, D.C., 2004**

Nota de Aceptación

Decano de la Facultad

Director del Proyecto

Jurado

Jurado

Bogotá D.C., de Octubre de 2004

Dedico con todo mi corazón el triunfo a:

DIOS

Quien siempre ilumina mi camino, me bendice y me conduce por la hermosa senda de la vida para desarrollar las potencialidades a través del estudio realizado

Con todo mi corazón para mis hijos:

Edwin Camilo Ceballos Sánchez: Mi hijo quien me brinda su confianza, ternura, colaboración y cariño.

Andrea Carolina Ceballos Sánchez, mi bebé quien con su cariño inmenso y ternura, me ha dado valor para no desfallecer.

A mis padres, quienes ven en mí uno de sus orgullos y les he cumplido, convirtiendo en realidad sus sueños, han logrado que mis metas no desfallezcan y han compartido conmigo mis angustias, alegrías, sueños y triunfos.

A mis hermanas: quienes con su paciencia y colaboración con mis hijos, lograron que se culminara esta meta.

Ruben Dario Marulanda que con su potencial de emprendedor, gran amigo, colega y compañero, logro que llegara al final de esta meta que nos habíamos propuesto desde que empezamos la carrera, me permitió crecer a su lado ERES GENIAL, nunca cambies.

Los amo.

AGRADECIMIENTO A LA COMPAÑERA

Ing. Emma Ramirez Cifuentes

Quien con su dedicación, conocimiento y apoyo logró que surgiera personal y profesionalmente en mi carrera.

MARTHA G. SANCHEZ VASQUEZ

A DIOS

Por darme la vida, la fe, la sabiduría y la salud para culminar con esta meta propuesta a través del estudio realizado.

A MI HIJA

Angie Estefany Marulanda Castañeda: mi linda niña, quien me brinda su ternura, siendo muy especial, cariñosa, y muy madura a pesar de su corta edad.

A MI MADRE

Quien con su constante estímulo, lograron en mi, la fortaleza para que este sueño se hiciera realidad.

AGRADECIMIENTOS A MIS AMIGOS

Compañera y camarada de estudio, quien con su colaboración y aliento no permitió que desfalleciera en momentos críticos durante el transcurso de la carrera.

Queremos dedicar de una manera muy especial a nuestra Coordinadora de carrera.

A los Ingenieros, Coordinadora de Proyecto y profesores de la Facultad de Ingeniería de Sistema de la UNAD. Que como amigos y docentes, logran dar a cada uno de sus estudiantes se fortalezcan en sus logros para alcanzar su meta profesional, que Dios la bendiga y les conserve por muchos años más en esta labor de enseñanza.

RUBEN DARIO MARULANDA

RESUMEN

Objetivo

El objetivo del proyecto es haber podido Recomendar y aportar al Grupo de Seguridad Informática de la Unidad Administrativa Especial de Aeronautica Civil (U.A.E.A.C), las herramientas necesarias del Plan de Continuidad de Tecnología, siendo necesaria su implementación y que sirva como soporte de diseño para la puesta en marcha del plan.

Metodología

El Grupo de Seguridad Informática de la Aeronáutica Civil Colombiana (UAEAC), no contaba con un sistema de plan de continuidad de tecnología que sirviera como soporte para aducir cualquier eventualidad de desastre, no se tuvo en cuenta ningún proceso de continuidad, para el desarrollo del plan de continuidad de tecnología; es necesario aclarar que únicamente se cuenta con un sistemas manual de aplicativos.

Resultados

Se garantiza el funcionamiento del plan de continuidad de tecnología y los mecanismos a seguir durante la duración de la eventualidad hasta la puesta en marcha del centro de cómputo alternativo off_site.

Lo anterior, da como resultado el funcionamiento en su totalidad del centro de cómputo alternativo, con más confiabilidad en la información.

CONCLUSION

Con el desarrollo del plan de continuidad de tecnología, se alerta a las directivas de la magnitud de las amenazas y riesgos a los que está expuesto el centro de cómputo de la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), los posibles desastres que se pueden presentar y formulando en la monografía las posibles alternativas de solución para que de esta manera se tomen las acciones previsivas antes de que ocurra un desastre.

TABLA DE CONTENIDO

CAPITULO I ASPECTOS GENERALES.....	12
1.1 PLANTEAMIENTO DEL PROBLEMA.....	12
1.1.1 FORMULACION.....	13
1.1.2 DELIMITACION.....	13
1.2 ANALISIS DE VARIABLES.....	14
1.3 OBJETIVOS.....	16
1.3.1 OBJETIVO GENERAL.....	16
1.3.2 OBJETIVOS ESPECIFICOS.....	16
1.4 JUSTIFICACION.....	16
1.5 HIPOTESIS.....	17
1.5.1 Hipotesis General.....	17
1.5.2 Hipòtesis de Trabajo.....	17
CAPITULO II MARCO DE REFERENCIA.....	18
2.1 MARCO TEORICO.....	18
2.1.1 ANTECEDENTES.....	20
3 MARCO CONCEPTUAL.....	21
4 MARCO HISTORICO.....	22
4.1 MARCO LEGAL DE LA AERONAUTICA CIVIL.....	24
4.1.1 Funciones a Unidad Administrativa Especial de Aeronàutica Civil	26
4.1.2 Funciones de la Direccìon de Informàtica	28
4.1.3 Funciones del Grupo de Soporte Informàtico	28
4.1.4 Funciones del Grupo de Sistemas de Informaciòn	29
4.1.5 Funciones del Grupo de Ingenieria y tecnologìa Informàtica	30
4.1.6 Funciones del Grupo de Seguridad informàtica	31
4.2 Descripciòn de los Sistemas de Informaciòn	31
4.2.1 Sistema ALDIA.....	31
4.2.2 Sistema PISTA.....	32
4.2.3 Sistema ESTADISTICAS DE TRANSPORTE AEREO.....	35
4.2.4 Sistema PAF.....	35
4.2.5 Sistema RECUESOS HUMANOS.....	36
4.2.6 Sistema SIGMA.....	37
5 CIENTIFICO.....	39
CAPITULO III METODOLOGIA DE DESARROLLO DEL PROYECTO....	39
1. TIPO DE INVESTIGACION.....	39
1.1 Alternativa de Trabajo.....	39
CAPITULO IV ETAPAS O FASES.....	40
1. Fase Exploraciòn.....	40
1.2 Tècnicas de Levantamiento de Informaciòn.....	41
1.2.1 Investigaciòn de Internet.....	41
1.2.2 Entrevistas no formales.....	41
1.2.3 Estudio de documentos de la Corporaciòn CANTV.	41
1.2.4 Observaciòn Directa.....	41
1.2.5 Conocimiento y Experiencia de trabajo en la Entidad	42
1.3 Riesgos que Podrian Subsanan el Impacto.....	42
2. Fase Anàlisis.....	42

2.1	Anàlisis de la Informaci3n.....	42
2.1.1	Operaci3n de Respaldo para los Proceso Cr3ticos.....	43
2.1.1.1	Centro de Procesamiento Alterno.....	43
2.1.1.2	Servicios de Hosting.....	44
2.1.1.3	Outsourcing.....	44
2.1.1.4	Servicios de Comunicaci3n.....	44
2.2	Definir los Procedimientos Alternos de Operaci3n.....	44
2.2.1	Operaci3n Automàtica.....	45
2.2.2	Operaci3n Manual.....	45
2.3	Identificaci3n de las características de un centro de procesamiento alternativo para recuperar la informaci3n y los aplicativos críticos.....	45
2.4	Identificar las operaciones alternas que deben desarrollarse para dar continuidad a los procesos.....	46
2.4.1	Sistemas de Informaci3n PAF.....	46
2.4.2	Sistemas de Informaci3n PISTA.....	46
2.4.3	Sistemas de Informaci3n ALDIA.....	46
2.5	Definir los procedimientos tècnicos de respaldo, recuperaci3n, reanudaci3n y restauraci3n de Hardware y Software para los procesos críticos.....	47
2.6	Definir los procedimientos de restablecimiento de los servicios de redes y telecomunicaciones del centro de computo alternativo..	47
2.6.1	Definici3n del equipo y plan de recuperaci3n a emergencias	47
2.6.2	Definir las posibles soluciones o respuestas de emergencia.....	48
2.6.3	Activa el Plan Jefe Grupo de Seguridad Informàtica	48
2.6.4	Definir los roles y responsabilidades ante una eventualidad de contingencia.....	49
2.6.4.1	Jefe Grupo Seguridad de Informàtica.....	49
2.6.4.2	Jefe de Soporte Informàtico.....	50
2.6.4.3	Administradores de Backups.....	51
2.6.4.4	Equipos de Emergencia.....	51
2.6.4.5	Definici3n del Plan de Recuperaci3n de Desastres.....	51
2.6.4.6	Identifica las Alternativas de Recuperar Recursos Tecnol3gicos Cr3ticos.....	52
2.6.4.7	Definir los procedimientos de recuperaci3n y reanudaci3n de servicios de redes y telecomunicaciones.....	53
2.7	Actividades requeridas para el anàlisis de impacto.....	54
2.8	IMPACTO OPERACIONAL EN LOS APLICATIVOS.....	54
2.8.1	Sistemas de Informaci3n ALDIA.....	55
2.8.2	Sistemas de Informaci3n PISTA.....	55
2.8.3	Sistemas de Informaci3n PAF.....	57
2.8.4	Sistemas de Informaci3n SIGMA.....	57
2.9	RIESGO DE APLICATIVOS.....	59
2.9.1	Terrorismo.....	60
2.9.2	Incendio.....	60
2.9.3	Actos de Sabotaje.....	61

2.9.4 Inundaciones.....	61
2.10 Determinación de Tiempos Limites de Interrupción.....	62
3. ANALISIS DE RIESGO.....	63
3.1 Identificación de Riesgo que pueden Afectar la Disponibilidad de la Plataforma Tecnológica.....	63
3.2 Evaluación de Riesgos.....	65
3.3 Conclusiones de Entrevistas Informales.....	68
3.3.1 Conclusión Entrevista Administrador Sistemas Operativos Windows 2000 Server.....	68
3.3.2 Conclusión Entrevistas Administrador Sistemas de Información PISTA.....	68
3.3.3 Conclusión entrevista Administrador Sistemas de Información ALDIA.....	69
3.3.4 Conclusión Entrevista Administrador Sistemas de Información PAF.....	69
3.3.5 Conclusión Entrevista Administrador Sistemas de Información MIGRAR.....	70
3.3.6 Conclusión Entrevista Administrador Internet.....	70
3.3.7 Conclusión Entrevista Lider Funcional Facturación.....	70
3.3.8 Conclusión Entrevista Lider Funcional Tesorería.....	70
3.3.9 Conclusión Entrevista Lider Funcional Facturación.....	71
3.3.10 Conclusión Entrevista Lider Funcional Presupuesto y Viáticos	71
3.3.11 Conclusión Entrevista Lider Funcional Módulo Administrativo..	71
3.3.12 Conclusiones con el Personal de Telecomunicaciones.....	71
Fase 3 Generar Recomendaciones.....	72
1. Centro de Barranquilla.....	72
2. Hosting.....	72
RECOMENDACIONES.....	74
CONCLUSIONES.....	75
GLOSARIO.....	76
ANEXO 1 Estructura Orgánica de Unidad Administrativa Especial de Aeronáutico Civil.....	80
ANEXO 2 Sistemas de Información y su Relación con las Dependencia de la UAEAC.....	81
ANEXO 3 Sistema de Información y su Relación con la UAEAC.....	82
ANEXO 4 Tabla Alternativa Centro de Computo.....	83
ANEXO 5 Sistemas de Información.....	83
ANEXO 6 Grafico Riesgo de Aplicativos.....	84
ANEXO 7 Matriz Riesgo de Aplicativos.....	85
ANEXO 8 Matriz Sistemas de Información.....	86
ANEXO 9 Identificación de Riesgos.....	86
ANEXO 10 Alternativa Centro de Computo alternativo.....	87
ANEXO 11 Costo – Beneficio.....	88
ANEXO 12 Cronograma de Actividades.....	89
ANEXO 13 Control Ingreso de Personal.....	90
BIBLIOGRAFIA.....	91

INTRODUCCION

Para la Unidad Administrativa Especial de la Aeronáutica Civil es de valiosa importancia diseñar, definir, desarrollar e implementar un Plan de contingencia de Tecnología Informática, que le permita garantizar continuidad en la prestación del servicio y en el funcionamiento de los sistemas de información que soportan las actividades diarias del negocio y es necesario contemplar el crecimiento de la Entidad en los últimos años.

Con este documento se pretende llevar a cabo el análisis y diseño de un Plan de contingencia de TI para los sistemas de información considerados críticos. En la actualidad la Entidad cuenta con un plan de contingencia manual para algunos sistemas de información, pero si se presentara algún desastre esto ocasionaría traumatismos en la operación normal y haría que prácticamente se paralizara por la cantidad de información que se genera y actualiza a diario.

Poner en marcha el plan de contingencia de TI, traería grandes beneficios para la Entidad tales como: continuar cumpliendo con sus obligaciones financieras y operativas en el tiempo indicado, garantizando el continuo recaudo que mensualmente esta al orden de los Treinta y Dos Mil Millones de pesos (32.000.000,00), aproximadamente, evitando así un caos financiero, además se evitaría que incurriera en demandas por el no cumplimiento de las obligaciones contraídas.

CAPITULO I ASPECTOS GENERALES

1.1 PLANTEAMIENTO DEL PROBLEMA

La Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), provee a sus usuarios internos y externos un sistema de información automatizado que permiten agilizar tareas administrativas, trámites y operaciones, estos aplicativos operan en una plataforma conformada por hardware y software de tecnología de punta en el mercado nacional e internacional. Cuando por alguna razón prevista o imprevista se afecta la disponibilidad del hardware y/o del software es necesario recurrir a un Plan de Contingencia Manual, que implica registrar en papel todas aquellas operaciones y transacciones que afecten el

.normal funcionamiento de la Entidad, tales como: pagos, registros contables, operaciones de aterrizajes y despegues de aeronaves, registros de sobrevuelos, registro de pasajeros exentos o que pagan tasa aeroportuaria, mantenimientos preventivos y/o correctivos a los equipos de ayudas a la navegación aérea, entre otros.

El plan de contingencia manual tiene debilidades tales como: falta de control de las operaciones registradas, duplicidad de registros, incremento del recurso humano, requiere invertir más tiempo en los procesos e incremento de costos de operación.

Debido a la necesidad de garantizar que los sistemas de información de la Unidad Administrativa Especial Aeronáutica Civil (UAEAC), tengan continuidad en caso de desastres o emergencias, es necesario desarrollar un proyecto que involucre este requisito fijando un norte en la eventualidad de presentarse un hecho de estos, teniendo en cuenta que nuestro país no es seguro por los problemas sociales, además de los riesgos y desastres naturales ocasionados por la posición geológica de la ciudad de Bogotá o provocados por agentes externos, por lo cual es fundamental para la Entidad que se garantice su funcionamiento implementando el Plan de Continuidad de Tecnología, que permita que la Entidad siga operando en un centro de procesamiento alternativo, mientras dure la emergencia utilizando hardware y software de iguales o superiores características a las requeridas en ambiente de normalidad.

1.1.1 FORMULACION

¿Si se implementa un Plan de Continuidad de Tecnología que contemple disponer de un centro de computo para procesamiento alternativo, se garantizará que la Unidad Administrativa Especial de la Aeronáutica Civil (UAEAC) continúe operando normalmente mientras dure la emergencia?

1.1.2 DELIMITACION

Nos ubicamos en la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC) situada en Bogotá, municipio de Cundinamarca, Aeropuerto El dorado, Edificio Centro Nacional de Aeronavegación, Piso 1, Dirección de Informática, Centro de Cómputo.

Para la prestación de sus servicios y el cumplimiento de sus obligaciones en el sector aeronáutico, la Unidad Administrativa de la Aeronáutica Civil (UAEAC) cuenta con diferentes sistemas de información que son administrados por personal de la Dirección de Informática, algunos de esos sistemas carecen de un plan de contingencia tecnológica, para atender los requerimientos en caso de desastres como incendio, inundación, terremoto, temblor y actos de sabotaje y/o terrorismo.

El proyecto contempla el respaldo que debe tener la Dirección de Informática de la Unidad Administrativa Especial Aeronáutica Civil (U.A.E.A.C.), en caso de presentarse un desastre en el Centro de Cómputo del CNA Piso 1, donde se encuentran ubicados los servidores de los sistemas de información: PAF, PISTA, ALDIA, SIGMA, RECURSOS HUMANOS, INTERNET Y SERVIDOR DE SERVICIOS DE RED WINDOWS Y CORREO ELECTRONICO, además de la infraestructura de las comunicaciones centrales que soportan los enlaces a los demás edificios del nivel central y la conexión con las regionales y aeropuertos del país.

Debido a lo extenso del alcance en este proyecto se realizara y documentará el Plan de Continuidad de Tecnología, la divulgación, entrenamiento y puesta en marcha del Plan de Continuidad de TI, será realizado por personal que delegue la Dirección de Informática de la Unidad Administrativa Especial de la Aeronáutica Civil (UAEAC), para tal fin.

1.2 ANALISIS DE VARIABLES

Los desastres que se van a contemplar y considerar en esta monografía si se materializan llegan a ocasionar interrupción de los servicios informáticos en la Unidad Administrativa Especial Aeronáutica Civil (UAEAC) y son:

Incendio

Ocasionado dentro del centro de cómputo, se dispersaría fácilmente, ya que el material del techo falso hace fácil combustión, este hecho originaría que las llamas se propaguen en un tiempo muy corto a los racks de los armarios de los servidores y sobretodo el cableado estructurado que es material muy

inflamable. Dando como resultado la pérdida de la comunicación de la red con todos los usuarios a nivel nacional.

Alrededor del centro de cómputo existen oficinas y el material en la que están construidas las paredes tales como cartón o madera son muy vulnerables ocasionando que las llamas se dispersen hasta el centro de cómputo y por consiguiente afectar los equipos.

Si no llega a afectar el centro de cómputo se quemarían algunas canaletas por donde va extendido el cable tanto eléctrico como de comunicaciones.

Inundaciones

Al llegar a materializarse, la infraestructura tecnológica de equipos situados en el centro de cómputo sufriría daños considerables y en la mayoría de los casos no se podrían recuperar por ser componentes electrónicos.

Temblor

La infraestructura del edificio no sufriría mayores daños, ya que el centro de cómputo no se vería muy afectado, el riesgo que se corre sería con las tabletas del piso falso que sobre éste reposan los servidores, es posible que se volteen los racks de los servidores y cableado principal. Pero un temblor de escala alta de acuerdo a las experiencias sólo se alcanza a mover el piso sin ocasionar ningún daño de equipos.

Terremoto

La infraestructura del edificio Centro Nacional de Aerovegación (CNA), donde esta ubicado el centro de cómputo si se llegara a presentar en una escala superior a 2 el desastre es devastador ya que la estructura de edificio no soportaría y se caería, dando como resultado pérdida de la infraestructura tecnológica existente.

Terrorismo

Si se coloca una bomba en algún lugar cercano con bastante carga la posibilidad que se derrumbe el edificio es comparada con un terremoto de magnitud alta y si se lanza un dispositivo perforaría las paredes ocasionando destrucción de la infraestructura y se generaría rápidamente fuego.

Sabotaje por acceso a la red de la Unidad Administrativa Especial de Aeronautica Civil (U.A.E.A.C).

Si se llegara a presentar, ocasionaría daño en librerías del sistema operativo Windows 2000 y podrían llegar hasta borrar carpetas de usuarios y aplicativos.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Analizar, Diseñar y Recomendar el **PLAN DE CONTINUIDAD DE TECNOLOGIA de la Unidad Administrativa Especial de Aeronautica Civil (U.A.E.A.C)**, como soporte con la coordinación y planificación de actividades que deben tener en cuenta la Entidad en caso de presentarse un desastre que afecte la continuidad de Tecnología Informática, aplicando las normas y políticas que garanticen la seguridad, confiabilidad y disponibilidad de la información.

1.3.2 OBJETIVOS ESPECIFICOS

- Explorar cuales son los sistemas de información críticos que requieren estar disponibles en caso de una contingencia de tecnología en la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC.)

- Analizar la información obtenida determinando la criticidad de los sistemas y posibles alternativas de solución.
- Recomendar el Plan de Continuidad de Tecnología para lograr la disponibilidad de los sistemas de información y los servicios informáticos requeridos.

1.4 JUSTIFICACION

En la actualidad la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), como entidad gubernamental cuenta con uno de los sistemas de información más robustos en el sector público, y por supuesto necesita cada vez más garantizar la continuidad del negocio que la soporta.

Con los avances tecnológicos que se cuentan y teniendo como punto de partida experiencias como las presentadas en Estados Unidos el 11 de septiembre del 2002, Aerocivil de Colombia no puede seguir sin tener un plan de contingencia, que garantice como mínimo operar sus sistemas de información, como lo son PISTA, ALDIA, SIGMA y PAF.

Al trabajar con un sistema automático a diferencia de hacerlo con un sistema manual el tiempo de respuesta se reduce considerablemente, además por la complejidad de los sistemas de información es más costosa la operación manual y no se obtiene la misma confiabilidad en los resultados.

1.5. HIPOTESIS

1.5.1 Hipótesis General

El Plan de Continuidad de Tecnología en la Unidad Administrativa Especial de Aeronáutica Civil (U.A.E.A.C), garantizará la continuidad del funcionamiento de las aplicaciones identificadas como críticas para la operación diaria de la Entidad

sin el temor del tipo de contingencia que se llegare a presentar, porque se tienen claramente definidas las actividades a seguir.

1.5.2. Hipótesis de Trabajo

Contar con la suficiente información interna y externa, debidamente analizada ya que será el insumo principal del Plan de Continuidad de Tecnología, además se deben tener en cuenta experiencias de situaciones similares ocurridas en otras empresas, con el fin de planear una estrategia válida que se acomode al entorno tecnológico y operativo de la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC).

CAPITULO II MARCOS DE REFERENCIA

2.1 MARCO TEORICO

Para entender el marco teórico es necesario contemplar los siguientes conceptos técnicos:

- **Plan de Contingencia**

La carencia del plan de contingencia ocasiona problemas de continuidad, al tener que actuar en caso de emergencia de manera no organizada lo cual puede ocasionar retraso en las operaciones propias de la Entidad frente a los demás entes del Estado y empresas particulares, entre ellas por ejemplo pérdida de tiempo en la elaboración de facturación manual, lo que genera altos costos de operación, ya que exige más recurso humano. Por lo tanto, sino se cuenta con un plan de contingencia de TI para afrontar una emergencia ocasionada por un desastre, la Entidad se ve expuesta a perder el control de la operación del día a día lo cual ocasionaría posibles problemas legales y altos costos de mantenimiento

al tener que operar de manera manual por un período de tiempo prolongado.

Se plantea como una posible alternativa contemplar un centro alternativo de procesamiento, ubicado en otra ciudad que soporte la operación mientras se restaura el sistema completo en el Nivel Central, sin que esto llegue a ocasionar grandes problemas a la Entidad. Se puede pronosticar que al entrar en funcionamiento el centro alternativo se puede seguir funcionando con las mínimas exigencias de sistemas de información por el tiempo mínimo de duración contemplado en el Plan de Contingencia para cada eventualidad.

Se enfocara principalmente en la restauración y puesta en funcionamiento de los sistemas de información PAF, PISTA, ALDIA y SIGMA, INTERNET, SERVIDOR SERVICIOS RED que son considerados como básicos requeridos para la continuidad de la operación de la Entidad.

- **Servidor**

Computador con características superiores, que debe tener más de un procesador y manejar varias tarjetas de comunicación a la vez etc., lo anterior, con respecto a las características que posee un computador personal normal. Su función principal es poder recibir y procesar requerimientos enviados desde una y/o varias terminales cliente/servidor conectados a una red.

- **Sistema de Información**

Es la agrupación de varios aplicativos y cada uno de ellos puede llegar a manejar diferente cantidad de módulos, una de las principales características de un sistema de información es que puede interactuar con otro u otros sistemas de información a través de interfaces (**tablas, archivos**), sin importar en que lenguaje de programación este desarrollado y cual sea la plataforma tecnológica que lo soporte.

- **Base de Datos**

Es una colección de datos que ofrece una presentación y estructura que permite un manejo más fácil y rápido de sus contenidos además de proporcionar nuevas facilidades para consultar, administrar y utilizar la información. Los datos se presentan de modo que el usuario pueda acceder directamente a ellos con la periodicidad que se ajuste más a sus requerimientos.

- **Servicio Informático**

Es el permiso de utilización de un componente tecnológico, bien sea de software o hardware que permite a un usuario conectado a la Red de la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), facilitar su trabajo en grupo para beneficio de la Entidad, son administrados por la Dirección de informática y son: el acceso a la red, el correo electrónico, la Intranet y el servicio de Internet.

- **Cluster**

Esta conformado por dos servidores, es decir, dos máquinas con las mismas características y que realizan las mismas funciones en estado activo/pasivo. Su función principal es que si se llega a caer el servicio de la maquina principal, la maquina secundaria toma el mando siendo transparente para el usuario este hecho, con el fin de no interrumpir la operatividad.

- **Servidor consolidador**

Es un servidor que permite la agrupación de varios sistemas de información con iguales o diferentes características de sistema operativo, donde se persigue que éste equipo ofrezca las mismas características de operatividad del equipo original donde se ejecutan las aplicaciones, sin importar la plataforma de sistema operativo.

2.1.1 ANTECEDENTES

En la Entidad no existe registro alguno de un Plan de Continuidad de Tecnología, afirmando que lo único que existe es un **plan de contingencia manual para aplicaciones**. El motivo que impulso a realizar el Plan de Continuidad de Tecnología Informática fue la probabilidad de ocurrencia de cualquier contingencia que se llegara a presentar en especial la situación social que se presenta en Colombia dado por el conflicto por grupos al margen de la ley y que la Unidad Administrativa Especial de Aeronáutica Civil (U.A.E.A.C), donde esta ubicado el centro de computo CNA (Centro Nacional de Aeronavegación) ubicado en Bogotá es muy vulnerable a cualquier tipo de ataque terrorista, Garantizando la disponibilidad y la oportunidad de la información ya que manualmente se demora más tiempo en obtenerla.

3 MARCO CONCEPTUAL

Se pretende describir y analizar los tipos de contingencias que se podrían presentar en la Unidad Administrativa Especial de Aeronáutica Civil (U.A.E.A.C), analizar el impacto financiero y operacional si se llegara a materializar una amenaza, formulando una solución viable para minimizar el problema presentado.

En el plan de contingencia de Tecnología Informática debe incluir el Plan de Continuidad y el Plan de Recuperación de desastres los cuales deben cumplir con los siguientes objetivos:

- Desarrollar y Recomendar estrategias y procedimientos que cumplan con los requisitos mínimos de operación y que con estos se pueda llegar a poner en operación los sistemas de información de la Unidad Administrativa Especial Aeronáutica Civil (UAEAC), definidos como críticos para la continuidad del negocio en el porcentaje óptimo requerido para su funcionamiento durante el tiempo que dure la contingencia.

- Desarrollar y Recomendar estrategias y procedimientos que permitan recuperar en un periodo predeterminado aceptable los recursos informáticos y de comunicaciones y restablecer el normal funcionamiento de los sistemas de información hasta lograr el 100% de operación una vez superada la contingencia.
- Asegurar que el Plan de Contingencia tenga un continuo cambio acorde con los cambios tecnológicos que se vayan presentando en los sistemas de información y que estén operando en producción antes del desastre.
- Mantener informado al personal de la Entidad de los procedimientos a seguir en caso de desastre, con el fin de que estén capacitados para actuar en el menor tiempo posible, creándoles conciencia del impacto que se tiene tanto a nivel personal como del funcionamiento de la Entidad, para poner en marcha.

4 Marco Histórico

Al fundarse en 1919 la primera Empresa Comercial de Aviación en el País, el Estado vio la necesidad de crear un organismo a cuyo cargo estuviera el control de la Aviación en todos los aspectos. Por medio de la ley 126 de 1919 se autorizó por primera vez al Poder Ejecutivo para que reglamentara todo lo relacionado con la Aeronavegación.

En un comienzo se creó la Comisión Técnica de Aviación para asesorar al Ministerio de Industria. Despacho al cual estaba adscrita la Aviación Civil; al trasladar el conocimiento de los problemas de Aviación al Ministerio de Guerra, se estableció una Dirección de Aviación.

La Ley 89 de 1938 centralizó el control de la aviación en un organismo especial denominado Dirección General de la Aeronáutica Civil, encargado especialmente de lo relacionado con los servicios de Aeródromos, rutas aéreas, radiocomunicaciones aeronáuticas, meteorología, vigilancia de personas, materiales e instalaciones destinados a la navegación aérea.

La Dirección General de la Aeronáutica Civil funcionó como Dependencia del Ministerio de Guerra de la Dirección General de la Aviación Militar.

Desde el año 1919 nuestro País es Miembro activo de los convenios Internacionales relacionados con la Aviación Civil. Es así como en la Convención realizada en Chicago en el año de 1944, se creó la Organización de Aviación Civil Internacional (OACI); este Convenio fue ratificado por el Congreso con la ley 12 de 1947; por el Decreto 969 de 1947, por el cual se reglamenta la estructura de la Aeronáutica Civil, adscribiéndola de nuevo al Ministerio de Guerra hasta el año de 1951, fecha en la cual se trasladó al Ministerio de Obras Públicas.

El rápido avance tecnológico hizo pensar en la necesidad de crear un organismo Nacional, encargado del control y prestación de servicios de Aeródromos y Aeronavegación para ejercer un control directo del espacio aéreo en razón de la seguridad que demanda la defensa de la Soberanía Nacional.

Para tal fin, la Nación optó por comprar los Aeródromos ya existentes, la mayoría de éstos de propiedad de Avianca, con todas las instalaciones de radioayudas de navegación y comunicación, además de la construcción y mantenimiento de nuevos aeropuertos y la adquisición de equipos de radioayudas y servicios aeroportuarios, para su normal funcionamiento.

Es así como el Gobierno Nacional en 1954, mediante Decreto 3269 del 10 de noviembre, creó el Instituto descentralizado denominado Empresa Colombiana de Aeródromos (ECA), encargado de la construcción, mejora y mantenimiento de los aeropuertos públicos, dotado de personería jurídica, autonomía administrativa y patrimonio propio.

En 1956 se adscribieron las funciones al Ministerio de Guerra. Posteriormente, con el fin de dotar a la autoridad aeronáutica de una autonomía administrativa y financiera se creó el Departamento Administrativo de Aeronáutica Civil (DAAC), mediante Decreto 1721 del 18 de julio de 1960, con unas funciones técnicas y administrativas específicas, para dirigir la política aeronáutica.

El Decreto 3140 de 1968 suprimió la E.C.A. y se creó en defecto el Fondo Aeronáutico Nacional "F.A.N.", establecimiento público adscrito al Departamento Administrativo de Aeronáutica Civil "DAAC". Mediante la Ley 3ª. y Decreto 2332 de 1977 se reorganizó el Departamento Administrativo de Aeronáutica Civil.

El Departamento Administrativo de Aeronáutica Civil y el Fondo Aeronáutico Nacional, en el año de 1984, determinaron un convenio con la Fuerza Aérea Americana, cuyo objetivo es establecer los términos y condiciones bajo los cuales la FAA proveerá ayuda al DAAC/FAN, para el desarrollo y modernización de la infraestructura de la Aviación Civil de la República de Colombia, en las áreas Gerencial, Operativa y Técnica.

Con la Ley 105 del 30 de diciembre de 1993, por la cual se organiza el Sector y Sistema Nacional de transporte adscribiendo nuestra institución al Ministerio de Transporte, como órgano rector de la política y ejecución de las funciones relativas al transporte aéreo; se diseñó un organigrama institucional que atiende a la naturaleza de las dos grandes tareas a la Entidad: la Aeronavegación y el servicio aeroportuario; en consecuencia se crean la Secretaria Técnico Aeronáutica y la Secretaria Aeroportuaria.

Esta Aerocivil es el resultado de la fusión del Departamento Administrativo de Aeronáutica Civil y el Fondo Aeronáutico Nacional, ordenado por el Art. 67 del Decreto 2171 de 1992.

4.1 Marco Legal de la AERONAUTICA CIVIL

La Unidad Administrativa Especial de Aeronáutica Civil -AEROCIVIL- es una entidad especializada, de carácter técnico adscrita al Ministerio de Transporte, con personería jurídica, autonomía administrativa y patrimonio independiente. Esta entidad es el resultado de la fusión del Departamento Administrativo de Aeronáutica Civil y el Fondo Aeronáutico Nacional, ordenada por el artículo 67 del decreto 2171 de 1.992.

La Aerocivil cuenta con regímenes especiales en materia de administración de personal, nomenclatura, clasificación, carrera administrativa, salarios, prestaciones y régimen disciplinario conforme a lo previsto en la ley 105 de 1.993 y las normas expedidas en desarrollo de la ley 4ª, de 1.992.

El régimen presupuestal y de contratación es el previsto para los establecimientos Públicos y en la ley 105 de 1.993.

Objetivo

La Unidad Administrativa Especial de Aeronáutica Civil tiene como objetivo garantizar el desarrollo de la aviación civil y de la Administración del espacio aéreo en condiciones de seguridad y eficiencia, en concordancia con las políticas, planes y programas gubernamentales en materia económico-social y de relaciones internacionales.

Misión

- Regular, administrar, planear y controlar el uso del espacio aéreo colombiano por parte de la aviación civil, y coordinar las relaciones de ésta con la aviación de estado, además, formular y desarrollar los planes, estrategias, políticas, normas y procedimientos sobre la materia.
- Garantizar el desarrollo ordenado de la aviación civil, la utilización segura y adecuada del espacio aéreo y contribuir al mantenimiento de la seguridad y Soberanía Nacional.
- Prestar los servicios de apoyo a la navegación aérea, aprovechando las ventajas competitivas del País y facilitando el transporte ínter modal, garantizando seguridad y oportunidad.

Visión

- Lograr un mejoramiento en el sistema de transporte aéreo del país, proyectando una positiva imagen en el mundo aeronáutico.
- La Aerocivil será una institución de gran calidad humana y amplia capacidad de trabajo; con una infraestructura potente y flexible, de tecnología moderna y con una organización eficiente y efectiva, integrada y coordinada bajo los parámetros nacionales e internacionales.

4.1.1 Funciones de la Unidad Administrativa Especial de Aeronáutica Civil - AEROCIVIL.

Son funciones generales de la Unidad Administrativa Especial de Aeronáutica Civil - AEROCIVIL, las siguientes:

Coordinar con el Ministerio de Transporte la definición de políticas y planes generales de aeronáutica civil y transporte aéreo, dentro del plan global del transporte, propendiendo por el desarrollo aeronáutico y aeroportuario del país.

Formular propuestas al Ministerio de Transporte para la definición de las políticas y planes generales de aeronáutica civil y transporte aéreo, dentro del plan global del transporte, propendiendo por el desarrollo aeronáutico y aeroportuario del país.

Garantizar el cumplimiento del Convenio de Aviación Civil Internacional y sus anexos.

Armonizar las disposiciones que promulgue la Organización de Aviación Civil Internacional con los Reglamentos Aeronáuticos Colombianos.

Dirigir, organizar, coordinar, regular técnicamente el transporte aéreo.

Controlar, supervisar y asistir la operación y navegación aérea que se realice en el espacio aéreo sometido a la soberanía nacional.

Promover e implementar estrategias de mercadeo y comercialización que propendan por el desarrollo, crecimiento y fortalecimiento de los servicios del sector aéreo y aeroportuario.

Desarrollar, interpretar y aplicar en todos sus aspectos las normas sobre aviación civil y transporte aéreo y ejercer vigilancia sobre su cumplimiento:

- Ejecutar las actividades necesarias para conformar, mantener, administrar, operar y vigilar la infraestructura aeronáutica y aeroportuaria que sea de su competencia.
- Expedir, modificar y mantener los reglamentos aeronáuticos, conforme al desarrollo de la aviación civil.
- Vigilar, evaluar y controlar el cumplimiento de las normas aeronáuticas y aeroportuarias en los aeropuertos propios, concesionados, descentralizados o privados.
- Propiciar la participación regional y los esquemas mixtos en la administración aeroportuaria.
- Intervenir y sancionar en caso de violación a los reglamentos aeronáuticos o a la seguridad aeroportuaria.
- Fijar y desarrollar la política tarifaria, en materia de transporte aéreo nacional e internacional y sancionar su violación.
- Desarrollar la política tarifaria, en materia de transporte aéreo y sancionar su violación.
- Establecer las tarifas, tasas y derechos en materia de transporte aéreo.
- Fijar, recaudar y cobrar las tasas, tarifas y derechos por la prestación de los servicios aeronáuticos y aeroportuarios o los que se generen por las concesiones, autorizaciones, licencias o cualquier otro tipo de ingreso o bien patrimonial.
- Dirigir, organizar, operar y controlar con exclusividad y en lo de su competencia, las telecomunicaciones aeronáuticas.
- Conducir en coordinación con el Ministerio de Relaciones Exteriores las relaciones con autoridades aeronáuticas de otros países y con organismos internacionales de aviación civil.
- Coordinar los lineamientos con las demás entidades u organismos que tengan a su cargo funciones complementarias con la aviación y el transporte aéreo.
- Propender por el perfeccionamiento, actualización y capacitación técnica del personal aeronáutico, conforme a los desarrollos tecnológicos.
- Realizar todas las operaciones administrativas y comerciales para el cabal cumplimiento de su objetivo.
- Fomentar y estimular las investigaciones en ciencia y en tecnología aeronáutica y aeroespacial.

- Facilitar la prestación de la asistencia técnica a las entidades de derecho público internacionales o de otros países que la soliciten, bajo acuerdos de cooperación bilateral o multilateral.
- Las demás que señale la ley de acuerdo con la naturaleza del modo de transporte.
-

Ver ANEXO 1. ESTRUCTURA Y ORGANIZACIÓN DE LA ENTIDAD

Ver ANEXO 2 ORGANIGRAMA DIRECCION DE INFORMATICA

Ver ANEXO 3 SISTEMAS DE INFORMACION Y SU RELACION CON LA UAEAC.

4.1.2 FUNCIONES DE LA DIRECCIÓN DE INFORMÁTICA

Planear, recomendar y desarrollar el crecimiento de la infraestructura informática de la entidad con los recursos tecnológicos avanzados.

Recomendar e implantar esquemas tecnológicos que agilicen o hagan más eficientes los procesos de la entidad.

Diseñar, desarrollar y mantener actualizados los sistemas de información y aplicativos de la entidad.

Prestar soporte técnico y operativo a los sistemas informáticos de la entidad.

Establecer las normas, estándares y recomendaciones técnicas para el manejo, control, seguridad y desarrollo de los sistemas de información y su infraestructura.

Crear y desarrollar los mecanismos para los casos de contingencias de los sistemas de información.

Asesorar y orientar en los asuntos propios de su competencia a la entidad.

Las demás que le sean asignadas de acuerdo con la naturaleza de la dependencia.

4.1.3 FUNCIONES DEL GRUPO SOPORTE INFORMATICO

Elaborar el plan nacional de operación y mantenimiento de los servicios informáticos que integran la infraestructura tecnológica informática aeronáutica y de gestión de recursos empresariales.

Organizar, supervisar y controlar la ejecución del plan de operación y mantenimiento de la infraestructura tecnológica informática aeronáutica y de gestión de recursos empresariales.

Prestar los servicios de soporte técnico informático de primer, segundo y tercer nivel a los usuarios de los sistemas de información aeronáuticos y de gestión de recursos empresariales.

Generar y Ejecutar los procedimientos de administración de los componentes tecnológicos informáticos aeronáuticos y de gestión de recursos empresariales.

Coordinar y Ejecutar las actividades necesarias para garantizar la prestación de los servicios informáticos.

Realizar los procesos de contratación de Mantenimiento y Conservación de los equipos que conforman la infraestructura tecnológica informática.

Garantizar la disponibilidad de la información mediante la correcta planeación, ejecución y control de las políticas de respaldo y recuperación.

Ejecutar el plan de contingencia para los sistemas de información aeronáuticos y de gestión de los recursos empresariales.

Realizar las labores de gerencia de proyectos, estableciendo mecanismos de seguimiento y control para el logro de los objetivos del proyecto.

Participar en conjunto con el grupo Seguridad Informática en la definición de las normas y procedimientos que garanticen la confiabilidad de la infraestructura tecnológica informática.

Ejecutar las recomendaciones generadas por el grupo seguridad informática para administrar la infraestructura tecnológica informática aeronáutica en producción.

4.1.4 FUNCIONES DEL GRUPO SISTEMAS DE INFORMACION

Realizar estudios de necesidades para la construcción y/o adquisición de nuevos sistemas de información aeronáuticos y de gestión de recursos empresariales.

Realizar la investigación, análisis, diseño, desarrollo, documentación e implementación de los sistemas de información aeronáuticos y de gestión de recursos empresariales.

Actualizar, afinar y mantener operativos los sistemas de información aeronáuticos y de gestión de recursos empresariales que se encuentran en producción en la Entidad.

Implementar y mantener actualizados los sistemas de información de gestión de recursos empresariales y los sistemas de información aeronáuticos necesarios para garantizar la seguridad aérea.

Establecer las normas, estándares y recomendaciones técnicas sobre los sistemas de información aeronáuticos y de gestión de los recursos empresariales.

Realizar el control de calidad de los sistemas de información aeronáuticos y los de gestión de los recursos empresariales.

Realizar las labores de gerencia de proyectos, estableciendo mecanismos de seguimiento y control para el logro de los objetivos del proyecto.

Evaluar permanentemente las nuevas tecnologías y herramientas computacionales para mejorar la calidad y el desempeño de los sistemas de información aeronáuticos y de gestión de recursos empresariales.

Participar en la definición de las normas, políticas, procedimientos y estándares de seguridad informática.

Ejecutar las recomendaciones generadas por el grupo seguridad informática en los sistemas de información aeronáuticos y de gestión de los recursos empresariales.

4.1.5 FUNCIONES DEL GRUPO INGENIERIA Y TECNOLOGIA INFORMATICA

Introducir los cambios tecnológicos necesarios para cumplir con los requisitos operacionales básicos para el intercambio de datos aeronáuticos, siguiendo los lineamientos de la OACI.

Participar activamente en los procesos de transición hacia los sistemas de Aeronavegación satelital.

Realizar las actividades conducentes a fomentar la evolución los sistemas de información aeronáuticos y de gestión de los recursos empresariales.

Realizar la ampliación y/o infraestructura tecnológica de los servicios informáticos.

Diseñar e implantar esquemas de redes que agilicen o hagan más eficientes los procesos aeronáuticos.

Investigar, Planear, Diseñar y Configurar la arquitectura de los componentes de la infraestructura tecnológica informática y telemática, teniendo en cuenta la evolución del sector aeronáutico.

Planear y Ejecutar conjuntamente con las demás áreas las tareas conducentes a brindar una optima infraestructura tecnológica para la prestación de los servicios aeronáuticos.

Definir y supervisar los procedimientos y estándares para la administración de los componentes tecnológicos.

Realizar los procesos de contratación para la adquisición de los sistemas y servicios informáticos que garanticen la operación aérea.

Realizar las labores de gerencia de proyectos, estableciendo mecanismos de seguimiento y control para el logro de los objetivos del proyecto.

Participar en la definición de las normas, políticas, procedimientos y estándares de seguridad informática.

Ejecutar las recomendaciones generadas por el grupo seguridad informática en la infraestructura tecnológica informática aeronáutica adquirida.

4.1.6 FUNCIONES DEL GRUPO SEGURIDAD INFORMATICA

Garantizar la integridad, exactitud y confidencialidad de la información aeronáutica y de gestión de recursos empresariales.

Definir, establecer y actualizar políticas, normas, procedimientos y estándares en materia de seguridad informática.

Evaluar, seleccionar e implementar herramientas que faciliten la labor de seguridad informática y contingencia para los servicios informáticos.

Participar en la definición, generación, implementación y pruebas del plan de contingencia para los servicios informáticos.

Realizar el análisis de riesgos de la infraestructura tecnológica informática aeronáutica.

Generar las recomendaciones pertinentes para garantizar la integridad, exactitud y confidencialidad de los sistemas de información aeronáuticos y de gestión de los recursos empresariales. Diseñar y establecer los estándares requeridos para optimizar los sistemas informáticos y garantizar la seguridad de la información.

4.2 DESCRIPCIÓN DE LOS SISTEMAS DE INFORMACIÓN

A continuación se describen brevemente los sistemas de información existentes en la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC): Ver anexi 3 Sistemas de información y su relación con las dependencias.

4.2.1 SISTEMA ALDIA

El Sistema de Información **A.L.D.I.A.** "Automatización en **L**ínea **D**e **I**nformación **A**eronáutica", provee una solución para la integración de la información en las áreas de la Subdirección General, la Oficina de Transporte Aéreo, la Oficina de Control y Seguridad Aérea y la Oficina de Registro de la Entidad.

Para alcanzar el objetivo de la Aeronáutica Civil, se hizo necesario contar con un Sistema de Información que permite el registro, la consulta y la actualización segura y en línea de la información relacionada con matrículas de aeronaves, aeronavegabilidad de aeronaves, personal aeronáutico, certificados médicos, pistas controladas, permisos de operación y funcionamiento de empresas de aviación, talleres de mantenimiento y centros de instrucción aeronáutica, a fin de garantizar el control y la regulación de la aviación civil en el territorio colombiano.

Se tienen registros históricos de un total de 4517 matrículas de aviones de las cuales están vigentes 1343. En la actualidad existen 688 aeronaves con certificado de Aeronavegabilidad vigente.

Versión Sistema Operativo:	Solaris 2.6
Versión Base de Datos:	Oracle 8.1.5.(se migrará a Oracle 9i)
Versión Herramientas de Desarrollo:	Developer 6i

El sistema de información ALDIA cuenta con los siguientes módulos:

- Aeronavegabilidad- CAE
- Empresas Talleres y Escuelas - CAM
- Licencias Aeronáuticas - CLH
- Medicina de Aviación - MAV
- Pistas y Helipuertos
- Registro Nacional Aeronáutico - RNA
- Módulos de Suspensión (4)
- Matriculas Extranjeras y sus permisos especiales
- Registro de Aeroclubes y suspensión de Ultralivianos
- Registro de Licencias Provisionales
- Tramite y Ejecutoria de Resoluciones

4.2.2 SISTEMA PISTA

PISTA es el proyecto que consiste en la integración técnica y funcional para los servicios de tránsito aéreo, las aplicaciones desarrolladas apoyan la función fundamental de la operación aérea en las torres de control y centros de control del país.

Tiene como objetivo proveer una herramienta que facilita la planeación, organización y optimización de los Servicios de Tránsito Aéreo, está integrado por los módulos de Horarios e Itinerarios, Planes de Vuelo RPL/FLP, Planes de Vuelo por Internet, Registro de operaciones de torres de control y centros de control, Documentos AIS (Control de NOTAM) y el Módulo de Administración.

El alcance nacional está dado por la implantación en todas las torres de control, de los diferentes aeropuertos, del módulo para el registro de las operaciones aéreas (aterrizajes y despegues) realizadas y que luego son transmitidas a nivel central en donde esos datos son la base para el proceso de Facturación de Servicios Aeroportuarios en el sistema PAF.

Este sistema permite:

- Recopilar la información correspondiente a la planeación, ejecución y apoyo de las operaciones aéreas.
- Controlar la información de transporte y asuntos internacionales en cuanto a rutas aprobadas, equipos, frecuencias de horarios e itinerarios, la asignación de slots y la recepción de los RPL's utilizados en la operación aérea.
- Controlar los planes de vuelo presentados en las Oficinas de Información Aeronáutica del País.
- Facilitar el registro y validación de Planes de vuelo por Internet mediante un formulario en la página www.aerocivil.gov.co.
- Generar automáticamente los FPLs a partir de los RPLs a nivel nacional.
- Registrar automática y manualmente las fajas de progreso de vuelo que se generan en las torres de control y los centros de control.
- Registrar y controlar los documentos publicados periódicamente por
- la Oficina de Información Aeronáutica, tales como NOTAM, Suplementos al manual AIP, Enmiendas al AIP y Circulares de Información Aeronáutica.
- Administrar en cuanto a parámetros y seguridad cada uno de los módulos del proyecto PISTA
- Completa integración de la información involucrada en la planeación, operación y estadística de Operaciones aéreas.
- Integración con otros sistemas de Información como ALDIA, PAF, FDPs
- Creación de las bases para la implementación del proyecto CNS/ATM
- Optimización de los servicios de tránsito aéreo.
- Confiabilidad y seguridad de la información para soportar la toma de decisiones.

Versión Sistema Operativo:	Solaris 9
Versión Base de Datos:	Oracle 9.2.0.4.
Versión Herramientas de Desarrollo:	Developer 6i.
Internet Application Server (IAS)	Release 1.

Módulos:

Torre de Control
Torre de Control - Históricos
Centros de Control
Centros de Control - Históricos
Documentos AIS
Plan Vuelo
Horarios e Itinerarios
Permisos Especiales de Vuelos
Estadísticas de Tránsito Aéreo
Estadísticas Regionales
Histórico Plan de Vuelo 1995-1998
Histórico Torre de Control 1995-1997

4.2.3 SISTEMA ESTADISTICAS DE TRANSPORTE AEREO

El Sistema de **ESTADÍSTICAS DE TRÁNSPORTE AÉREO**, permite llevar un registro estadístico de las diferentes variables del transporte aéreo tales como: Pasajeros, carga, correo, servicios aeroportuarios y cursos de instrucción.

Este sistema permite el cargue automático o manual de información, facilitando el intercambio de información con las empresas aéreas, mantiene un registro histórico para facilitar la generación de variables estadísticas y dispone de herramientas que facilitan el análisis estadístico del transporte aéreo.

Versión Sistema Operativo:	Solaris 9
Versión Base de Datos:	Oracle 9.2.0.4
Versión Herramientas de Desarrollo:	Developer 6i Cognos BI

4.2.4 SISTEMA PAF

El sistema de información **PAF** es el sistema de apoyo a las labores de Planeación, Administración y Financiera de la Entidad, dándole una herramienta de información Gerencial a la alta Dirección para la toma oportuna de decisiones, basándose en la información en tiempo real suministrada por el sistema. Para la implementación del PAF se adquirió la tecnología ERP y e-business.

Para el sistema PAF se realizó la implementación del **ERP PeopleSoft** (antes JDEdwards) con los módulos Financiero, Abastecimientos y Comercial; la implementación del aplicativo **Charrycs** (en Visual FoxPro) con sus módulos Planeamiento, Presupuesto y Viáticos; y la implementación del aplicativo **Porfin – Portafolio Financiero** con sus módulos de Tesorería, Caja, Deuda, Inversión y Conciliación, todos sobre el manejador de base de datos ORACLE.

Versión Sistema Operativo:	HP-UX 11i
Versión Base de Datos:	Oracle 8.1.7.4 (se migrará a 9i)
Versión de Software:	PeopleSoft (antes JDEdwards) ERP 8.0
Service Pack 22 Update 1	
ALFA GL Versión 4.0 - Developer 6i	
CHARRYCS Foxpro Versión 5.0	

4.2.5 SISTEMA DE RECURSOS HUMANOS

EI SISTEMA DE RECURSOS HUMANOS tiene como objetivo permitir el control y administración de la planta y manejo de la información del personal de la Entidad desde su ingreso, todas sus novedades administrativas hasta su retiro, así como del proceso de nómina y prestaciones sociales. Todo bajo las normas vigentes para las entidades oficiales y más específicamente para la Aeronáutica Civil.

En los 25 principales aeropuertos del país, está siendo consultada la información del módulo de administración de personal y nómina. Adicionalmente ingresan las novedades para el proceso de Horas Extras.

Los datos para la Evaluación de Desempeño son digitados semestralmente en las Regionales y en el Nivel Central.

Versión Sistema Operativo:	Solaris 2.6
Versión Base de Datos:	Oracle 8.0.5.
Versión Herramientas de Desarrollo:	Forms: 5.0.6.8
	Report: 3.0.5.8.0
	Pro*C: 4.1.

4.2.6 SISTEMA SIGMA

El proyecto SIGMA, Sistema de Información para la Gestión de Mantenimiento Aeronáutico, es un sistema de apoyo que permite registrar las labores de mantenimiento de equipos con el fin de tener la supervisión y control de estaciones aeronáuticas, sistemas, equipos, herramientas y/o repuestos, así como del factor humano del sector de soporte técnico aeronáutico para lograr una adecuada planeación y programación de los mantenimientos preventivos y correctivos y así establecer indicadores y estadísticas de gestión.

El sistema permite la gestión de actividades diarias de mantenimiento como mecanismo de mejoramiento continuo, además permite el análisis de rutinas de identificación de averías repetitivas en los equipos, análisis eficiente de causas y registro de las acciones correctivas tomadas para la prevención de nuevos fallos. Este control de la información permitirá mejorar la eficiencia

de las acciones de mantenimiento planificado y lograr incrementos de productividad significativos.

Versión Sistema Operativo:	Solaris 9
Versión Base de Datos:	Oracle 8.1.7. (se migrará a 9i)
Versión del Software:	MAXIMO Versión 4.1.1

Módulos que maneja:

- Solicitudes
- Diagnostico
- Planificación y seguimiento
- Programación y asignación
- Suministro de combustible
- Ordenes de trabajo
- Mano de obra
- Planes
- Seguridad
- Trabajo
- Inventarios
- Configuración
- Recursos
- Mantenimiento preventivo
- Informes
- Equipos
- Interfaces
- Solicitudes: Genera las diferentes órdenes de trabajo para el sistema (OT).
- Diagnostico: Evalúa el diagnostico del tipo de solicitud para enlutarlo.
- Planificación y seguimiento: Determina que OT requiere la orden de trabajo a realizar como tiempo viáticos, materiales etc.
- Programación y asignación: Asigna el recurso humano y técnico requerido para hacer el trabajo.
- Suministro de combustible: Maneja la disponibilidad de combustible requerido para tener operativa la infraestructura aeroportuaria en todos los aeropuertos.

- Ordenes de trabajo: **M**aneja las diferentes órdenes de trabajo generadas en el sistema.
- Mano de obra: **A**signa la mano de obra requerida para ejecutar el trabajo incluyendo precios de viáticos.
- Planes: hace la planificación de las ordenes de trabajo determinando como que y cuando realizar.
- Inventarios: Muestra y asigna la disponibilidad de material a utilizar confrontando con las existencias y el almacén donde se encuentra.
- Configuración: configuración del sistema
- Recursos: Asigna los recursos necesarios humanos y técnicos para realizar el trabajo.
- Mantenimiento: no de los equipos.
- Informes: Maneja los diferentes reportes de los módulos existentes.
- Equipos: Contiene la información técnica de los equipos incluyendo fotos de este de los componentes que lo integran.
- Interfaces: Hace interfaces preventivo: Controla la información de toda la infraestructura tecnológica, identificando los tiempos de hacerle mantenimiento a cada con los diferentes módulos y sistemas de información de la entidad que requiera para su funcionamiento.

5 CIENTIFICO

De acuerdo al análisis del diseño del plan de contingencia, se logra establecer un método científico de ejecución de dicho procedimiento fijando políticas exactas para llegar a operar, al presentarse una contingencia de forma ordenada, segura y en un tiempo mínimo, sin que haya mayor traumatismo en la operación diaria de la Entidad.

Lo anterior, se logra llevando paso a paso todas las etapas del proyecto hasta su culminación, tomado como referencia la documentación de los diferentes portales de Internet y entrevistas con los diferentes administradores del sistema de información y líderes funcionales, ya que con ésta se logrará establecer una bitácora para la documentación de dicho plan.

CAPITULO III METODOLOGIA DE DESARROLLO DEL PROYECTO

1. TIPO DE INVESTIGACION

El tipo de investigación a realizar en la presente práctica empresarial es de ingeniería aplicada, ya que en ella se ponen en práctica y se aprovechan los conocimientos y las experiencias adquiridas durante la etapa de formación académica.

1.1 ALTERNATIVA DE TRABAJO

El presente trabajo es de tipo Práctica Empresarial, ya que el propósito es Recomendar el Plan de Continuidad de Tecnología para la Unidad Administrativa Especial de Aeronáutica Civil (U.A.E.A.C), tomando como base la documentación existente en la Entidad y tomar como referencia la documentación publicada en los diferentes portales de Internet de empresas especializadas en el tema, con el fin de llegar hasta la parte de desarrollo, mas no documentar la parte de implantación y puesta en marcha ya que esta etapa se encarga la firma que gane la licitación para tal propósito.

CAPITULO IV ETAPAS O FASES

1. Fase Exploración

Recopilación de Documentación

En esta recopilación de la documentación existente en la Entidad, se analiza con el fin de planificar la estrategia a seguir para el desarrollo del proyecto, además la documentación externa que servirá para ayudar a documentar y adaptarlas.

La información que posee la Dirección de Informática, es la bitácora de los Sistemas de Información en cuanto al Software y Hardware que tiene la Entidad y que es base fundamental para dimensionar el proyecto.

La recopilación de toda la información que sirve como referencia para documentar el plan de continuidad tecnológica para la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), se basa en las siguientes actividades:

- Investigar información relacionada con planes de contingencia y recuperación de desastres.
- Clasificar y analizar la información recopilada
- Definir el alcance del plan de continuidad de TI
- Definir los requerimientos del plan de continuidad de TI
- Analizar la situación actual de tecnología
- Realizar un paralelo entre requerimientos vs. condiciones técnicas y operativas para proporcionar la situación esperada de continuidad de tecnología.

1.2 Técnicas de Levantamiento de Información

Tiene el propósito de hacer levantamiento de la información existente en la Unidad Administrativa Especial de Aeronáutica Civil (U.A.E.A.C.), en los diferentes portales de Internet y en las compañías relacionadas con el tema de tecnología informática y planes de contingencia.

1.2.1 Investigación en Internet: Para conocer el avance en el tema de continuidad de tecnología a nivel mundial y analizar las experiencias encontradas.

1.2.2 Entrevistas no formales: Se realizaron entrevistas verbales a los diferentes responsables de los componentes tecnológicos involucrados

1.2.3 Estudio de documentación de la Corporación CANTV:

Lectura del documento de Procedimiento para la Continuidad del Negocio y Recuperación de Desastres de la Corporación CANTV de fecha 01.03-2002.

1.2.4 Observación directa: La atención al usuario mediante la línea helpdesk, para contabilizar el tiempo de respuesta en caso de una eventualidad; para concluir la efectividad de actuar ante un riesgo.

1.2.5 Conocimiento y Experiencia de trabajo en la Entidad: Los sistemas de información, los componentes de hardware y software de la UAEAC debido a las labores realizadas en función del cargo desempeñado.

1.3 Riesgos que Podrían Subsanan el Impacto

Para analizar el riesgo del impacto se va a tener en cuenta la siguiente lista:

1. Realizar el análisis de impacto para los diferentes servicios y procesos informáticos de la UAEAC (Unidad Administrativa Especial Aeronáutica Civil).
2. Clasificar los sistemas de información en producción en la UAEAC (Unidad Administrativa Especial Aeronáutica Civil), dependiendo de su criticidad e impacto así:
 - Criticidad A: Aplicaciones que necesariamente deben ejecutarse, la interrupción permitida no deberá ser mayor a 48 horas.
 - Criticidad B: Aplicaciones que admiten una interrupción definida en el tiempo y/o pueden ser reemplazadas parcial y temporalmente con procedimientos manuales.
 - Criticidad C: Aplicaciones que permiten una interrupción prolongada sin causar impacto.

3. Determinar los tiempos límites aceptables de interrupción.
4. Identificar los elementos de Hardware y Software que soportan los procesos críticos de negocio.
5. Identificar el impacto financiero y operacional de la ocurrencia de una amenaza.
6. Clasificar el impacto financiero y operacional.
7. Identificar los cinco (5) procesos críticos de la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), según su impacto financiero y operacional identificando criticidad A, B y C.

2. Fase Análisis

2.1 Análisis de la información

El análisis de la información, es aquella que sirve como base para la conclusión del desarrollo del presente proyecto en la Unidad Administrativa Especial de Aeronáutica Civil (U.A.E.A.C). y se tendrán en cuenta las siguientes conclusiones:

El plan de contingencia estará enfocado a reestablecer únicamente los aplicativos mencionados en la fase uno que son PAF, PISTA, ALDIA, MIGRAR e INTERNET, es decir montar la infraestructura necesaria de tal manera que soporte los sistemas de información considerados como críticos para la entidad. Bien sea que si se llega a presentar una catástrofe que pueda soportar la operación de estos mediante una de las cuatro (4) opciones siguientes que soportan los procesos críticos:

2.1.1 Opciones de Respaldo para los Procesos Críticos

- Centro de procesamiento alternativo
- Servicios de Hosting
- Servicios Outsourcing
- Servicios de comunicaciones

2.1.1.1 Centro de Procesamiento Alterno: Se recomienda la regional Barranquilla, por poseer la infraestructura y ser el segundo centro de control del país (Ver anexo 4 tabla Alternativa Centro de Cómputo), debido a que los costos son superiores y se debe tener en cuenta un lugar adecuado para el montaje del mismo y además duplicar todos los servidores del centro de cómputo principal que tenga que ver con el plan de continuidad de tecnología.

Las actualizaciones se pueden hacer de inmediato o en paralelo sin tener que esperar que el tiempo sea definido por terceros y fácilmente se logre ampliar el plan para nuevos sistemas de información de acuerdo a necesidades futuras; esto da como resultado costos más bajos, a pesar de las ventajas descritas en esta numeral se adiciona la desventaja de asumir costos superiores por cambio de tecnología de hardware no siendo rentable porque el software de actualización siempre requiere de hardware de superior performance, quedando en obsolescencia en corto tiempo el existente.

2.1.1.2 Servicios de Hosting: Este tipo de servicio es el recomendado en la práctica empresarial por las características del ambiente de la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC).

La Entidad está en la obligación de actualizarse constantemente a nuevas versiones de software de acuerdo a las exigencias de los proveedores de aplicativos de desarrollo, ya que estos no dan soporte sino hasta máximo tres (3) versiones anteriores del producto, pero cuando sea necesario actualizar debe planearse conjuntamente el proveedor de Hosting, requiriendo de mayor tiempo para ejecutar la actualización. Los centros de procesamiento de Hosting normalmente tienen varios clientes y necesariamente deben estar cambiando de tecnología en un tiempo más corto que cualquier empresa porque deben mantener el negocio en el futuro para garantizar el servicio a sus clientes.

Es necesario dejar una cláusula cuando la Unidad Administrativa Especial de Aeronáutica Civil (U.A.E.A.C), llegue a efectuar el contrato, donde se estipule concretamente la obligación por parte del proveedor que garantice la actualización de hardware acorde a las

futuras exigencias de los sistemas de información contemplados en el plan de continuidad de tecnología de la Entidad.

2.1.1.3 Outsourcing: La posibilidad se descarta por cuanto la Entidad cuenta con personal técnico capacitado para la administración de la información y del centro de cómputo alternativo si se llegara a implantar como solución.

2.1.1.4 Servicio de Comunicaciones: Para este tema se puede pensar en contratar un enlace con una compañía que preste dicho servicio, esta solución se toma solo en el caso de quedar deteriorado el canal de comunicación LAN TO LAN.

2.2 Definir los procedimientos alternos de operación:

Operación automática

Operación manual

2.2.1 Operación automática: Este tipo de procedimiento es el ideal para el plan de contingencia de TI ya que es el perseguido por el presente documento implementado de acuerdo a las recomendaciones descritas.

2.2.2 Operación manual: En caso de no poner en funcionamiento el plan de forma automática total o parcialmente de los sistemas de información es necesario suplir la necesidad con un plan manual de cada uno de los aplicativos o mixto mientras se puede levantar el centro de cómputo principal.

2.3 Identificación de las características de un centro de procesamiento alternativo para recuperar la información y los aplicativos críticos

Cualquiera de las alternativas que se escoja como la aceptada para operar el Plan de Continuidad de Tecnología, es necesario que cuente con las siguientes características mínimas de operación:

Preferiblemente tener instalaciones físicas en cualquiera de las regionales descritas anteriormente de infraestructura tecnológica o servicio de Hosting.

Centro de cómputo que mantenga en funcionamiento los servidores y la infraestructura de comunicaciones con el nivel central con características de servidores consolidados.

- **Instalaciones físicas:** Estas deben estar acondicionadas físicamente para soportar y mantener la infraestructura informática requerida, además las comunicaciones deben ser optimas entre los enlaces LAN to LAN.
- **Centro de cómputo:** Debe estar dotado con los servidores descrito para soportar el Plan de Continuidad de Tecnología y el hardware de comunicaciones para establecer el enlace con centro de compute principal (Bogotá).

2.4 Identificar las operaciones alternas que deben desarrollarse para dar continuidad a los procesos.

2.4.1 Sistema de información PAF

Se deben instalar los aplicativos en cada uno de los PCs que estén definidos para el proyecto y deben tener instalado lo siguiente:

JDEdwards versión 7334

Instalar acceso directo del aplicativo Charry que se conecte con el servidor de aplicaciones.

Instalar acceso directo del aplicativo Alfagl

Adicionalmente cada uno de los PCs deben tener instalado sistema operativo Windows 2000 profesional, Microsoft Outlook, Oracle 9i; la

configuración de estas maquinas debe ser Pentium IV con disco duro mínimo de 20 GB y memoria Ram 128 mínimo.

2.4.2 Sistema de información PISTA: Encargándole de manejar horarios itinerarios, ingresar las fajas de vuelo de los centros de control del país, expedir las bitácoras de planes de vuelo, sacar estadísticos de vuelos nacionales e internacionales de aeronaves que sobre vuelan el espacio aéreo internacional, dar permisos especiales para aeronaves que deben hacer un vuelo en un tiempo no establecido en un plan de vuelo. Se deben instalar los aplicativos en cada uno de los PCs que estén definidos para el proyecto, debe poseer oracle 9i, y el mismo hardware de los demás sistemas de información contemplados en el plan.

2.4.3 Sistema de información ALDIA : Lleva el registro de aeronaves tanto privadas como comerciales, llevar el control de la empresa, talleres y escuelas, se mantiene el control de licencias técnicas tanto de vuelo como tierra del personal aeronáutico, Medicina registro y control de los certificados médicos expedidos por los delegados, En aeronavegabilidad se analiza la investigación de accidentes de aeronaves, efectuando la parte legal y operativa de estas, además se hacen suspensiones por no pago a la entidad de los diferentes empresas que hacen uso del espacio aéreo y talleres arrendados. Se deben instalar los aplicativos en cada uno de los PCs que estén definidos para el proyecto, debe poseer oracle 9i y el mismo hardware de los demás sistemas de información contemplados en el plan.

2.5 Definir los procedimientos técnicos de respaldo, recuperación, reanudación y restauración de Hardware y Software para los procesos críticos.

- Sistema de información PAF: Mirar procesos actuales de procedimientos técnicos de respaldo, recuperación, reanudación y restauración de Hardware y Software

- Sistema de información PISTA: Mirar procesos actuales de procedimientos técnicos de respaldo, recuperación, reanudación y restauración de Hardware y Software
- Sistema de información ALDIA: Mirar procesos actuales de procedimientos técnicos de respaldo, recuperación, reanudación y restauración de Hardware y Software.

2.6 Definir los procedimientos de restablecimiento de los servicios de redes y telecomunicaciones del centro de cómputo alternativo.

2.6.1 Definición del equipo y plan de recuperación a emergencias (responsables).

El equipo de trabajo debe estar conformado por las siguientes integrantes:

Director de informática
Jefes Grupos Dirección de informática
Administrador de soluciones informáticas
Lideres funcionales
Personal delegado de la dirección de telecomunicaciones
Personal delegado por la dirección de desarrollo aeroportuario

2.6.2 Definir las posibles soluciones o respuestas de emergencia

Las posibles soluciones a la solución de emergencia, están dadas de acuerdo a la magnitud presentada por el desastre presentado, pero es importante definir dentro de las tres alternativas presentadas cual es la más viable para la Entidad, mirando todos los pro y contra que tiene cada alternativa.

Establecer el equipo de respuesta a emergencias. El personal que conforme este equipo debe ser idóneo en toma de decisiones, es decir debe ser muy calificado y conocedor del entorno global que lo rodea y específico en su área.

La escala debe ser definida de acuerdo a los siguientes perfiles para realizar las tareas secuencialmente.

2.6.3 Activa el Plan Jefe Grupo Seguridad Informática

Evalúan el desastre los diferentes jefes de grupos de la dirección de informática conjuntamente con los delegados de la dirección de telecomunicaciones y dirección de desarrollo aeroportuario.

Activan la puesta en marcha el grupo de administradores de los sistemas de información.

Ejecutan el plan de trabajo los diferentes líderes funcionales y están en continua comunicación con los diferentes administradores de las sistemas para ajustar en el menor tiempo posible el sistema.

Los líderes funcionales conjuntamente con los administradores ajustan el sistema para poner a trabajar los usuarios finales.

El equipo de emergencia en general esta a la guardia de lo que sucedo para escalar los problemas presentados a la persona que tenga que dar solución a este.

2.6.4 Definir los roles y responsabilidades ante la eventualidad de una contingencia

2.6.4.1 Jefe de Grupo Seguridad Informática:

- Programa y ejecuta coordinadamente con las áreas involucradas, la revisión anual de las operaciones normales, respuestas de emergencia, procesamiento y almacenamiento y recuperación de la tecnología informática.
- Revisa, pruebas y modifica procedimientos y sistemas de seguridad física y lógica según sea requerido.
- Solicita auditorias sobre procesos, revisiones y pruebas.
- Se encarga de activar el plan, coordina con el equipo de emergencias el plan a seguir para reestablecer el funcionamiento en el menor tiempo posible y mantiene actualiza la lista del personal involucrado con direcciones de residencias y teléfonos para poder ubicarlos inmediatamente las 24 horas del día de los 365 días del año.
- El jefe de grupo de soporte informático conjuntamente con los administradores de los sistemas de información anualmente o de acuerdo a las necesidades realiza pruebas de funcionamiento del sistema e integridad del mismo.
- El jefe de grupo de soporte informático garantiza el procesamiento y almacenamiento de la información en cualquier momento que se requiera, para esto debe estar informándole a diario la persona que este encargada de los backups de lo ocurrido haciendo pruebas continuas para garantizar la restauración en el centro alterno off-Site.
- El equipo de plan de desastre evalúa de forma practica el Plan de Continuidad de Tecnología Informática, solicita al jefe de grupo soporte informático el reporte de backups con la información contenida en cada una de ellas.

- Anualmente realiza pruebas de respuesta en el sitio off-site y de integridad de información, actualiza con los requerimientos de infraestructura, para prevenir emergencias en caso de verse inaccessibles.

2.6.4.2 Jefe de Soporte Informático

Se encarga de mantener actualizado los reportes para almacenamiento y reajuste de equipos en el sitio off-side y debe manejar la información del centro de cómputo así:

- Aire acondicionado (marca/modelo/vendedor)
- Electricidad (entrada/salida/potencia)
- Especificaciones de los servidores(marca/modelo/vendedores)
- Equipos periféricos(marca/modelo/vendedores)
- Telecomunicaciones y redes(marca/modelo/vendedores)
- Líneas telefónicas(marca/modelo/vendedores)

2.6.4.3 Administradores de Backups

Se encarga de realizar los backups diarios, semanales, mensuales, semestrales y anuales de estos en el sitio Off_Site.

Mantiene actualizado los procedimientos de restauración de información de los servidores del sitio off-side.

2.6.4.4 Equipo de Emergencia

- Planifican, participan, y ejecutan revisiones y pruebas de acceso a información respaldada, pruebas de directrices especiales y estrategias interinas de procesamiento y almacenamiento.
- Definición de políticas, normas y procedimientos necesarios para delegación o designación de actividades al equipo de respuesta a emergencias.
- La respuesta a emergencias identifica tareas y responsabilidades requerida para activar el plan en el momento de un desastre específico que ocurra.
- Establece la capacidad de procesamiento y almacenamiento de datos en el momento en que ocurra un desastre.
- Contacta el personal de respuesta a emergencias que trabajara individual o colectivamente durante el periodo que dure la respuesta a emergencias, todo lo anterior de acuerdo a lo establecido por el director de informática.

2.6.4.5 Definición del Plan de Recuperación de Desastres

En el momento de presentarse el desastre se deben realizar consecutivamente y cronológicamente los pasos siguientes :

Evaluar la magnitud del desastre, en cuanto a operatividad del centro de cómputo, infraestructura y pérdida humana de quienes deben participar en el plan.

Activar el plan de acuerdo a lo establecido por la magnitud de este.

Restaurar las bases de datos con el último backup obtenidos antes del desastre.

Activar la red para poner a trabajar los usuarios.

Mirar el comportamiento del procesamiento a medida que entran los usuarios y hasta obtener un porcentaje óptimo de carga de usuarios.

Empezar a restaurar el centro de cómputo central.

Restaurar la base de datos del centro de computo principal con los backups obtenidos del centro de computo off-side.

Hacer pruebas de integridad antes de activar los usuarios en el centro de computo reestablecido.

Activar los usuarios en el centro de computo original

Mirar el comportamiento de hardware y software con la carga de usuarios.

Desactivar los usuarios del sitio Off_Side.

2.64.6 Identificar las Alternativas para Recuperar los Recursos Tecnológicos Críticos.

Las alternativas viables son :

- Servicios de Hosting
- Definir los procedimientos de recuperación de Hardware y Software que soporta procesos críticos.
- Identificar el tipo de pérdida presentada, teniendo en cuenta que si llega a involucrar hardware es necesario evaluar la reinstalación del sistema operativo; es necesario hacer este paso primero que todo.
- Hacer la restauración de la información perdida por cualquier razón.

- Si no es necesario reinstalar sistema operativo, se hace la restauración del último backup de información o del export si es Base de Datos.
- Identificar el tipo de hardware dañado evaluándolo si es servidor o equipo de comunicaciones.
- Servidor: activar el plan de continuidad de acuerdo a las recomendaciones para tal caso y llamar a los proveedores para reposición.

El Equipo de comunicación: Evaluar la zona o el sector afectado por la pérdida y activar las comunicaciones que se tengan para emergencia en cada caso.

2.6.4.7 Definir los procedimientos de recuperación y reanulación de servicios de redes y telecomunicaciones.

En caso de afectar el tipo de desastre las instalaciones del centro de computo del Centro Nacional de Aeronavegación (CNA), debe activar el Switch de respaldo ubicado en el centro de cableado del edificio Eldorado en la ciudad de Bogotá 5to piso, que tiene los puertos para recibir el enlace de Fibra Óptica conectado LAN TO LAN con el centro de procesamiento alternativo definido como Off_Side, se deben realizar secuencialmente los siguientes pasos.

Avisar al encargado de telecomunicaciones para activar la red alterna de microondas con el centro de procesamiento Off_Side Conectar a la red el Switch de nivel 3 (enrutador).

Conectar servidores y enrutadores desde el centro de computo Off_Side LAN TO LAN.

Verificar los tiempos de respuesta con los servidores.

Verificar los tiempos de respuesta con la carga de usuarios trabajando.

Ajustar las fallas de tiempos.

2.7 A continuación se muestran las principales actividades requeridas para el análisis de impacto:

1. Identificación de riesgos
2. Evaluación de riesgos
3. Asignación de prioridades a las aplicaciones
4. Establecimiento de los requerimientos de recuperación
5. Elaboración de la documentación
6. Verificación e implementación del plan
7. Distribución y mantenimiento del plan

Se hace necesario identificar los procesos críticos para el análisis del impacto financiero y operacional determinando los tiempos límites aceptables de interrupción.

ANEXO 5. Sistemas de Información y su relación con las dependencias de la Unidad Administrativa Especial de Aeronautica Civil (UAEAC).

2.8 IMPACTO OPERACIONALE EN LOS APLICATIVOS:

El impacto operacional de la Unidad Administrativa Especial de Aeronautica Civil (UAEAC) en caso de verse afectada la plataforma tecnológica que soporta los sistemas de información se verán reflejados así:

2.8.1 SISTEMA DE INFORMACIÓN ALDIA

Si no se puede actualizar la base de datos no se tiene información en línea de:

- **Módulo Registro:** Se le estaría dando carta abierta a los morosos de las aeronaves por consiguiente no se estarían inhabilitando las aeronaves para poder volar.
- **Módulo Aeronaves:** No se recaudaría el cobro por los diferentes servicios de comunicación prestados en vuelo a las aeronaves.
- **Módulo Empresas:** Las obligaciones de las empresas aéreas pendientes con la Aeronautica no podrían controlar y estas podrían volar libremente sus aeronaves sin ser multadas por la AEROCIVIL.
- **Módulo Medicina:** Sería difícil controlar la validez de los certificados médicos del personal de vuelo.
- **Módulo Licencias:** No se podría verificar el estado de las licencias y chequeos de pilotos que los habilita para su función, con respecto a solicitudes que efectúan las empresas o entidades estatales para investigaciones judiciales.
- **Moduló Investigación de Accidentes:** No teniendo las pruebas suficientes recopiladas por este grupo. No se podría dictaminar la causa ni tampoco el responsable de este.

2.8.2 Sistema de Información PISTA

- **Módulo Planes de Vuelo: Internet y Normal:** La aprobación de un Plan de vuelo depende de la vigencia de las licencias y certificados médicos del personal de vuelo y su certificado de Aeronavegabilidad, si esto no está en línea, se podrían cometer fraudes. (Volar aeronaves suspendidas con personal de vuelo no autorizado). Seria el mas críticos de todos los módulos porque si no se puede desarrollar la actividad diaria llegaría a afectar notoriamente después de 96 horas el modulo de facturación en PAF.
- **Módulo Horarios Itinerarios:** No se podrían capturar las operaciones de transporte aéreo que son la información de las obligaciones de las empresas transportadoras, los itinerarios de vuelos de las diferentes compañías aéreas, las rutas de las aeronaves que deben seguir en vuelo, los horarios asignados para volar en el país, la información de los equipos (aeronaves) que están autorizados para trabajar.

- **Módulo Torre Centros de Control:** No se alimentaría el sistema con la información de las fajas (información de las aeronaves en vuelo) que generan los controladores de los vuelos de entrada y salida de los aeropuertos.
- **Módulo Aprobación Planes de Vuelo:** La información de los planes de vuelo que se generan a diario no se realizaría.
- **Modulo Aisaro:** No se tendría información en medio magnético de los notams (información de las eventualidades que se presentan en los aeropuertos a nivel nacional) como son cierres de aeropuertos, daños en ayudas etc.
- **Módulo Estadísticas** No se podrían efectuar las estadísticas de las empresas aéreas, como la cantidad de operaciones en un tiempo determinado y cantidad de pasajeros transportados etc.
- **Módulo Permisos Especiales:** No se podrían otorgar permisos a las diferentes aerolíneas que operan en el territorio nacional para volar en un tiempo determinado, o realizar algún evento determinado transitorio en un tiempo. Ej. Operar vuelos charter adicionales.
- **Módulo Usuarios y Permisos:** No se tendrían las autorizaciones especiales para realizar algún trabajo determinado en plataforma o en vuelo.
- **Operaciones Aéreas:** No se podrían registrar los vuelos diarios de las aeronaves que cruzan el espacio aéreo nacional ni tampoco las autorizaciones de vuelos.

2.8.3 SISTEMA DE INFORMACIÓN PAF

- **JDEdwards:** No se podrían hacer operaciones de compra adquisiciones, arriendos, cobranzas, cuentas por pagar, cuentas por cobrar, contabilidad, inmuebles, facturación, contratos y activos fijos.

- **Módulo Cobranzas:** La Entidad dejaría de facturar y recaudar las obligaciones que tiene con sus clientes por diferentes motivos, tampoco no se podría hacer la interfase con el modulo Pista para actualizar el registro de las aeronaves que están parqueadas en plataforma y detectar cuanto tiempo deben de arriendo para poder hacer el respectivo recaudo por la Unidad Administrativa Especial de Aeronautica Civil.(U.A.E.A.C).
- **Presupuesto:** No se podría hacer reasignación de rubros a las diferentes actividades, por consiguiente la Entidad se vería afectada en las diferentes actividades de pago, no se podrían hacer registro presupuéstales, esto ocasionaría que las obligaciones de pagos se demoraran, por consiguiente se presentaría mora hacia los proveedores por no pago a tiempo.
- **Viáticos:** Se generarían hechos cumplidos en viáticos y seria necesario recurrir a elaborar resoluciones motivas.
- **Tesorería:** No podría efectuasen los diferentes pagos a los diferentes compromisos adquiridos por la Entidad y tampoco se podrían recibir pagos en caja, de los clientes.

2.8.4 Sistema de Información SIGMA

No podrían generar órdenes de trabajo (OT), para viaticar los técnicos, que deben cubrir el mantenimiento de las operaciones aéreas a nivel nacional, ya que es necesario hacer interfase con la base de datos de nomina, viáticos y JDEdwards.

La Unidad Administrativa Especial de Aeronautica Civil (**U.A.E.A.C**), carece de un plan de continuidad de tecnológica que garantice la continuidad de operación en los sistemas de información considerados como más críticos. Siendo la dificultad mayor el definir un centro de computo de procesamiento alterno, bien sea de propiedad exclusiva de la Entidad o prestado por alguna de las figuras que existen en el mercado como son Hosting, Housing o Outsourcing.

¿Si se materializa un riesgo que se debe hacer?

Identificar el tipo de riesgo, dentro de los analizados para la contingencia.

Seguir el plan de acuerdo a las instrucciones del documento del plan de contingencia.

¿Que pasaría a futuro con el Plan de contingencia?

Con el fin de garantizar la operatividad y funcionalidad del Plan de Contingencia, éste debe ser actualizado cada vez que se presente cualquier tipo de cambio en los sistemas de información o se realice una actualización a nivel del hardware o de la infraestructura tecnológica.

¿Que resultados se obtienen al aplicarlo?

La continuidad en el funcionamiento de los sistemas de información sin presentarse grandes traumatismos.

Recuperación de infraestructura tecnológica en caso de desastres al saber como actuar de manera organizada en un tiempo mínimo.

Experiencia para futuros desastres del mismo tipo o diferente, al aplicar experiencias anteriores y actualizar el documento Plan de Contingencia.

Estabilidad financiera para la Entidad y continuidad en la operación sin mayor impacto a nivel nacional.

Asignación de prioridades en las aplicaciones

” Después de que se materialice un riesgo y se inicie la recuperación de los sistemas, se debe saber qué aplicaciones recuperar en primer lugar. No hay

que perder el tiempo restaurando los datos y sistemas equivocados cuando la actividad empresarial necesita primero sus aplicaciones esenciales.”

Esto implica la necesidad de determinar por anticipado cuáles son las aplicaciones fundamentales del negocio.

Los sistemas de información en producción en la UAEAC (Unidad Administrativa Especial Aeronáutica Civil), se clasifican dependiendo de su criticidad e impacto así:

http://www.iin.oea.org/manual_proyectos.PDF

2.9 RIESGO APLICATIVOS

Ver ANEXO 6 Grafico Riesgos Aplicativos

- **Criticidad A:** Aplicaciones PAF, PISTA, ,
- **Criticidad B:** Aplicaciones recursos humanos, etc.
- **Criticidad C:** Aplicaciones ALDIA

Ver ANEXO 7 Grafico Matriz Riesgos de Aplicativos

2.9.1 Terrorismo : Se clasifica en nivel de riesgo 2 porque se tiene vigilancia privada en la entrada del edificio CNA y el control que realizan los vigilantes no permiten el ingreso de vehículos o personal que no esté debidamente autorizado. Si se requiere el ingreso de personal diferente a funcionarios se debe autorizar este previamente por un funcionario de la Entidad y los vehículos que ingrese son inspeccionados visualmente.

La vulnerabilidad esta presente en la circulación de vehículos por la Avenida Eldorado.

- **Frecuencia:** La probabilidad que ocurra es alta ya que no se puede controlar el flujo vehicular por la avenida Eldorado. La probabilidad

que ocurra es dos (2), debido a estar tan cerca de la avenida del edificio CNA. (Centro Nacional de Aeronavegación).

- **Impacto financiero** : Es alto debido a que si se llega a materializar el tipo de acto en la Unidad Administrativa Especial de Aeronautica Civil (U.A.E.A.C), dejaría de recaudar cada día un promedio de mil millones de pesos.
- **Impacto operacional:** Es medio debido a que existe la posibilidad de trabajar manualmente mientras se puede restaurar los sistemas de información.

2.9.2 Incendio el nivel de riesgo es mínimo debido a los controles existentes que se poseen.

- **La frecuencia** que ocurra es mínima debido a que se tienen detectores de incendios en el centro de computo y extintores en este para evitar la propagación y en general en todas las oficinas de la Entidad, pero principalmente cuenta con bomberos disponibles las 24 horas del día que son funcionarios de la Empresa y la distancia del sitio donde operan al centro de computo se puede garantizar que en un termino de 3 a 5 minutos puede llegar al sitio.
- **Probabilidad de ocurrencia** es mínimo debido a que en el centro de computo las maquinas permanecen a temperaturas bajas por tener un buen aire acondicionado y nuevo además de no se utiliza maquinaria que disipe bastante energía.
- **El impacto financiero** seria mínimo de acuerdo a las seguridades que existen para evitar este tipo, si llegara a ocurrir muy probablemente se podrían salvar los equipos o gran parte de ellos.
- **Impacto operacional** es alto porque seria necesario arreglar la parte dañada y esto puede tardar más de 48 horas por ser muy

dispendioso el trabajo además de ser impredecible que se puede afectar.

2.9.3 Actos de sabotaje: Es de tipo medio ya que no esta exento, aunque el personal que tiene acceso al centro de cómputo es muy reducido tanto para trabajar a nivel de software o hardware a éste.

- **Frecuencia:** Es media debido a que se tienen controles tanto físicos como de software que controlan este evento además que históricamente la frecuencia por parálisis de actividades de tipo sindical son mínimas.
- **Probabilidad de ocurrencia:** Es medio debido a los controles establecidos.
- **Impacto financiero :** El análisis es medio de las variables anteriores.
- **Impacto operacional:** Es alto debido a que si se llega a presentar este acto seria ejecutado por alguien que conoce cómo afectar la operación por largo tiempo.

2.9.4 Inundación Es baja debido a que el centro de cómputo esta en el primer piso del edificio CNA y este esta elevado de la base aproximadamente 4 metros, por el área del centro de cómputo no atraviesan desagües ni tubos de agua que afecten este.

- **Frecuencia:** Es baja debido a la topología del terreno y la construcción del edificio.
- **Probabilidad:** De ocurrencia mínima, por no existir ductos por encima o por las paredes que afecten el área del centro de cómputo.
- **Impacto financiero** Es alto debido a que el agua afectaría fácilmente el hardware siendo una de las principales causa de daño severo por ser circuitos electrónicos.
- **Impacto operacional:** Es alto debido a que el tiempo que transcurre en reparar o reponer maquinaria puede ser superior a 48 horas.

2.10 Determinación de Tiempos Limites de Interrupción

Anexo 8 Matriz Sistemas de Información

Las matrices reflejan el comportamiento en caso de presentarse algún tipo de desastre los sistemas de información de JDEdwards, el tipo de impacto es alto, para todos los módulos que lo conforman, para Charry y presupuesto es el mismo comportamiento.

Para el sistema de información PISTA es bajo, soportaría hasta un mes trabajando manualmente excepto los módulos de digitación de torres de control y planes de vuelo siendo más crítico, en escala; en la torre se empezaría a general un problema serio después de 96 horas sin operar automáticamente por la cantidad de información.

El tiempo de interrupción para todos los módulos de JDEdwards es de 24 horas, para presupuesto y Charry es de 12 horas o menos, para pista soportan una interrupción superior de una semana y es considerado como crítico después de 96 horas para los dos módulos descritos anteriormente.

La criticidad en general sería de tipo medio para el sistema de información PISTA.

El sistema de información ALDIA se puede manejar con un plan de continuidad manual, actualmente se tiene implementado trabajar con el último reporte del día anterior, pero la veracidad es máximo de 96 horas, de ahí en adelante se torna crítico ya que no habría como obtener este informe nuevamente.

El impacto financiero para todos los módulos de JDEdwards es alto.

El módulo de presupuesto es alto y para viáticos alto.

Para PISTA es medio y Para ALDIA medio.

La clasificación para los sistemas de información financiero y operacional de JDEdwards es alto, para presupuesto es alto, para viáticos medio, para PISTA medio, para sigma alto y ALDIA medio

3 ANÁLISIS DE RIESGOS

Se analizarán los riesgos, identificando los que pueden afectar la disponibilidad de la plataforma tecnológica, evaluando el impacto de las amenazas críticas a la que se esta expuesta, los componentes tecnológicos críticos de software y hardware relacionados con los riesgos y controles existentes, las vulnerabilidades de los controles si se materializan las amenazas y analizando los riesgos tecnológicos y los requerimientos mínimos relacionados con hardware y software que soportan las operaciones de la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC).

3.1 Identificación de Riesgos que Pueden Afectar la Disponibilidad de la Plataforma Tecnológica

Hace referencia a tres simples preguntas: ¿qué está bajo riesgo?, ¿qué puede ir mal? y ¿cuál es la probabilidad de que suceda?

En la evaluación realizada en la Entidad los riesgos definidos como posibles son aquellos que se pueden llegar a presentar de acuerdo a las características del país como:

- Terrorismo
- Incendio
- Actos de sabotaje
- Inundación
- Temblor y
- Terremoto

Los cuales se conceptúan de la siguiente manera:

Terrorismo: Se da por la situación de conflicto por parte de los grupos al margen de la ley que existen y estos acostumbran colocar bombas o disparar artefactos explosivos en cualquier parte del país, donde lo que buscan es desestabilizar la columna vertebral de la democracia colombiana.

Incendio: En Bogotá, a pesar que el clima es frío, no esta exento que se origine un incendio de cualquier magnitud.

Actos de sabotaje: Es común que se presente en cualquier organización empresarial, debido a la diversidad de intereses que hay por parte de grupos de individuos o personas que buscan cubrir algún tipo de falta o hacer protagonismo de violar la seguridad de una infraestructura o un sistema de información.

Inundación: Ninguna organización es infalible a que se presente este tipo de contingencia, aunque sea en menor grado por desastre natural o por accidente.

Tembor: En general en el mundo es probable que se llegue a presentar este hecho, sin poder predeterminar la escala de desastre que llegue a presentar.

Terremoto: Es el extremo del temblor y se mide de acuerdo a la magnitud que presentada, siendo devastador por debilitar la infraestructura.

Ver anexo 9 Tabla Identificación de Riesgos

3.2 Evaluación de Riesgos

En el caso de los servicios informáticos y los sistemas de información, la preocupación principal es determinar la pérdida financiera y el impacto operacional que puede provocar la interrupción de los servicios, teniendo en cuenta:

a) Incendio

En el centro de computo la probabilidad que exista un incendio es baja debido a que hay instalados detectores de humo, cámaras de vigilancia y personal de vigilancia las 24 horas, además se cuenta con una estación de bomberos ubicada en el Aeropuerto, la cual tiene un mecanismo de conexión con el centro de computo que puede identificar en cualquier momento alarma de incendio.

Sin embargo, aunque la probabilidad es baja, si se materializa este tipo de amenaza, lo más probable es que se afecten las comunicaciones y en casos extremos y los servidores que soportan los sistemas de información.

b) Terrorismo

La probabilidad que se presente un acto de terrorismo esta catalogado como en ALTA, a pesar que el aeropuerto cuenta con buena seguridad por parte de vigilancia privada y funcionarios de cámara, pero la reacción de la policía es deficiente por tardar demasiado tiempo en reaccionar, lo cual da como resultado el incremento de puntos vulnerables como son:

- Fácilmente se puede dejar cargas explosivas en sitios estratégicos, en especial en las entradas, baños , sitios de espera de los muelles nacional e internacional del edificio Eldorado y puente aéreo, además a los alrededores del edificio CNA, ALMACEN, CEA y bodegas de carga y descarga de mercancías.
- El tiempo que transcurre en reaccionar la policía después de ser avisado por el funcionario encargado de cámaras del CNA es de 10 minutos, lo cual da un margen suficientemente extenso para hacer detonar una bomba desde un vehículo que se deje estacionado hasta 300 metros de diámetro alrededor del CNA ya que se encuentra en la mitad de la entrada y salida de la avenida 26, siendo extremadamente vulnerable para un acto terrorista.

c) Sabotaje a la red de información por acceso a la red interno y externo.

El nivel de sabotaje que se tiene en la empresa, se puede catalogar como bajo, debido a que se tiene buenas medidas de control, porque se cuenta con herramientas que garantizan y controlan las entradas mediante el software antivirus de Mcafee que se llama SpamKiller y se encuentra instalado en el servidor mercurio el cual esta en la zona desmilitarizada y la función es realizar el chequeo mediante lista de intrusos, detectando que información tiene y las características para entrar al servidor de correo en Internet, y los que no tiene permiso sencillamente no los deja entrar. La información que deja entrar es filtrada y la recibe el servidor de correo BOG1, que se encarga de hacer otro filtrado antes de ser entregada al usuario final.

Adicionalmente, se tiene el control mediante consola ya que si algún usuario entra por algún dispositivo bien sea disquete o CD y el contenido de este logra infectar el PC, el software detecta inmediatamente y avisa a los diferentes servidores del evento impidiendo el acceso del PC infectado al dominio. La acción es que una vez detectado por el administrador de antivirus avisa al helpdesk para que sea desinfectado el PC.

A nivel de correo se cuenta con antivirus Mcafee con el producto Groupshield, la función de este es actualizar automáticamente a diario los nuevos virus que están saliendo en el mercado, aunque no se descarta del todo que se pueda infiltrar un troyano. Además el puerto 80 que sirve de entrada y salida a Internet tiene los controles necesarios.

Si se dejan huecos de seguridad en cuanto a permisos a usuarios indebidos para poder instalar localmente en las máquinas software, la posibilidad es mayor de ataque por virus.

La utilización de módems en los computadores portátiles esta prohibido y controlado por parte de informática, de tal forma que quien traiga un portátil y quiera conectarlo a la red, no lo puede hacer por no tener permisos de acceso.

Los ataques posibles en la red se presentan por petición al servidor por DOS (Denial Of. Service) y consiste en que simultáneamente se piden demasiados acceso desde afuera y esto podría bloquear el servidor de Internet.

Actualmente, se esta trabajando en implementar software que hace chequeo de filtrado de contenido para evitar básicamente que aquellas direcciones que tiene que ver con pornografía, terrorismo, juegos, música, etc., las logre detectar y así poder restringir el acceso de los usuarios a estas.

d) Sabotaje por ingreso al centro de cómputo

Para el acceso al centro de cómputo se controlado por una puerta que se mantiene constantemente cerrada y la entrada a éste es permitido a un grupo reducido de funcionarios de informática, el ingreso de personal ajeno debe ser autorizado por el jefe del área y se debe registrar en la planilla de control de los funcionarios **Ver F01 CONTROL DE INGRESO PERSONAL.**

3.3 Conclusiones de Entrevistas Informales

Los administradores de sistemas de información concuerdan en que no existe ningún plan de continuidad de tecnología a la fecha, solo existe plan de contingencia para recuperación de aplicativos de forma manual.

3.3.1 Conclusión Entrevista al Administrador Sistema Operativo Windows 2000 Server.

Llamado BOG2, éste es el servidor principal de dominio de los demás servidores que existen en AEROCIVIL, se encarga de administrar todas las cuentas de los 2400 usuarios de la U.A.E.A.C., además sirve de servidor de servicios WIN (resuelve los nombres de usuarios) y DNS (Domain Network System). Existen en cada regional un servidor por cada

una de ellas que se encarga de resolver el nombre y hacer interfase con el servidor principal para la validación.

Existen tres maquinas configuradas en cluster que son BOG1 como dominio principal y BOG10 y BOG11 que hacen de backups de BOG1, la función de estos es asignar las direcciones a las maquinas de usuarios, en caso de presentarse falla en el principal entra a funcionar uno de los secundarios.

Los servidores BOG3 ubicado en el Edificio Eldorado oficina 502, BOG2 ubicado en el centro de cómputo del edificio CNA y BOG8 ubicado en el edificio CEA, hacen la función de servidores WINS para cada edificio. El servidor BOG hace de Sysinf (acceso de aplicaciones de desarrollo).su función es permitir que usuarios que trabajan en desarrollo establezcan login con éste.

3.3.2 Conclusión Entrevista Administrador Sistema de Información PISTA

En la actualidad la Entidad tiene implantado este sistema en veintiséis (26) aeropuertos del país, con el fin de controlar las operaciones aéreas.

Se cuenta con un plan de contingencia de aplicativos para operar manualmente, con el fin de suplir las necesidades hasta un máximo de 96 horas, de ahí en adelante se determina como critico, ya que afecta la facturación por no poder incluir las fajas de vuelo generadas a diarios por aterrizajes y despegues de aeronaves.

El servidor ATS maneja la Base de datos, si al pensar en tener un centro de computo alterno en otra ciudad de propiedad de la U.A.E.A.C se podría mantener tecnológicamente mientras no se migre a la ultima versión de Oracle 10G y esto puede tardar alrededor de tres (3) años o mas, una vez se necesite hacer la migración la maquina no esta en capacidad de soportar la versión debido a que necesita 3 GB de memoria RAM como requerimiento de Oracle.

3.3.3 Conclusión entrevista administrador sistema de información ALDIA

En la actualidad se cuenta con un plan de contingencia de aplicativos y consiste en sacar un reporte diario al finalizar cada día, en caso de tener que operar manualmente es utilizado para verificar la información suministrada por los usuarios, pero este únicamente es confiable hasta 96 horas después, pasado este tiempo pierde toda fiabilidad por movimiento de información que se presenta en el sistema.

Además existen usuarios internos y externos como son Fuerza Aérea de Colombia, sedes en Bogotá y Barranquilla, Dirección Nacional de Estupefacientes y Policía Nacional.

3.3.4 Conclusión Entrevista Administrador Sistema de Información PAF

El sistema de información es bastante pesado de ahí que es necesario tener maquinas Pentium III y IV para que opere en optimas condiciones, ya que este es el motor de la Dirección Financiera, dando la alternativa de operar manualmente en un determinado tiempo, este sistema maneja todas las ordenes de compra y facturación, hacerlo manualmente por mucho tiempo no es confiable por la gran cantidad de ordenes que se efectúan a diario, esto ocasiona que cuando se restaure el sistema tardaría bastante tiempo en alimentarlo de nuevo.

3.3.5 Conclusión Entrevista Administrador Sistema de Información MIGRAR

Al materializarse un desastre se dejarían de hacer ordenes de trabajo y se perdería el control de los mantenimientos que se deben efectuar diariamente en las diferentes estaciones de radioayudas, no se tendría el control de los viáticos porque no se lograría hacer interfaz con el modulo de presupuesto, personal y contabilidad.

3.3.6 Conclusión Entrevista Administrador Internet

Internet y correo electrónico se han convertido en una cultura en la empresa y si no existe un plan de continuidad tecnológica para estas, la U.A.E.A.C se vería expuesta a que si se llegara a presentar un desastre no se puedan publicar las páginas a las que por ley todas las entidades gubernamentales deben editar las licitaciones para adquisición de cualquier bien.

3.3.7 Conclusión Entrevista Líder Funcional Facturación

El tiempo máximo de operación sin sistema es de 12 horas de ahí en adelante se torna crítico debido a que la facturación no tiene espera, se dejaría de enviar las facturas a los clientes en las fechas establecidas y ocasionaría demoras en los pagos.

3.3.8 Conclusión Entrevista Líder Funcional Tesorería

Al trabajar manualmente ocasiona demoras, ya que el cliente debe subir al quinto piso donde queda facturación y pedir su estado de cuenta para su cancelación posterior.

3.3.9 Conclusión Entrevista Líder Funcional Facturación

Si se llegara a presentar una contingencia en el Módulo de Información de facturación se atrasaría el envío de correspondencia a los clientes y no habría manera de decirles cuál es el valor que debe pagar, por tal razón afectaría el módulo de tesorería en las cajas a nivel nacional.

3.3.10 Conclusión Entrevista Líder Funcional Presupuesto y Viáticos

Al no poder trabajar en presupuesto ocasionaría problemas con el sistema de información de tesorería, por no poder definir cuánto es el

pago que deben efectuarse debido a las obligaciones contraídas con terceros por parte de la U.A.E.A.C, esto causaría sanciones para la empresa generando hechos cumplidos en presupuesto; de igual manera no se podrían crear viáticos para el personal que debe cumplir funciones en otros aeropuerto, siendo estos vitales para la operación de la Entidad.

3.3.11 Conclusión Entrevista Líder Funcional Módulo Administrativo

Se acumularía información y atraso en los procesos, por tener que realizar doble función, como es un proceso manual y posteriormente incorporarlo en el sistema. Tomándose como crítico después de dos (2) semanas por la cantidad de órdenes acumuladas para ingresar al sistema.

3.3.12 Conclusiones con el Personal de Telecomunicaciones

Las posibles centro de procesamiento serían en orden de importancia la ciudad de Barranquilla en el Aeropuerto Ernesto Cortizos, por el ser el segundo centro de control más importante del país, ya que este cuenta a diferencia de los demás con la segunda antena satelital después de la Regional Bogotá, con este se podría garantizar que en caso de fallar las comunicaciones de microondas el canal se habilite para transmisión de datos para que opere por satélite.

Como segunda opción se tendría la regional Aeropuerto Alfonso Bonilla Aragón de la ciudad de Cali, este por tener a nivel de microondas un solo salto en su topología. Además que actualmente se tiene arrendado con Telecom la red de microondas ya que las radioayudas de la Aeronautica Civil, fueron destruidas por grupos al margen de la ley, pero el seguro de éstas debe hacer reposición, dejándolas funcionando con la misma operatividad que se tiene las arrendadas actualmente.

Fase 3 Generar Recomendaciones

Las alternativas más viables son:

1 Centro Barranquilla

Porque la entidad tiene definido y operando como centro de control secundario para la navegación aérea nacional y radioayudas a nivel nacional e internacional el aeropuerto Ernesto Cortizos de la ciudad de Barranquilla, y se cuenta con una amplia infraestructura de telecomunicaciones y cuenta únicamente con dos saltos en la red de microondas (a mayor altura la comunicación se hace más estable). Además físicamente el aeropuerto cuenta con mayor espacio físico para albergar el hardware requerido (anexo Centro de computo alterno). Por no disponer actualmente del hardware requerido seria necesario hacer una inversión de tecnología.

2 Hosting

No se invertiría en infraestructura tecnología de servidores, por no asumir costos de instalación y adecuación del centro de cómputo, se mantendría salvaguardada la información.

Los costos de mantenimiento se reducen por el hecho de mantener en buen estado operativo el enlace con el sitio Off_Side definido.

Los precios de actualización de plataforma tecnológica donde residen los aplicativos resultan más económico por ser compartido con los demás usuarios que utilizan el servicio, adicionalmente se obtiene mayor fiabilidad de recuperación de la información.

Obtener mejores precios del servicio ya que el centro de cómputo de la U.A.E.A.C. se encuentra ubicado sobre la Avenida 26 siendo esta una red

de información adaptada por varias empresas que prestan servicios de comunicación en el país.

Ver Anexo 10 tabla Costo-Beneficio

RECOMENDACIONES

- Mantener actualizado el Plan de continuidad del negocio y recuperación de desastres así como, las aplicaciones que soportan dichos procesos, antes que ocurra un desastre.
- Las operaciones normales requieren tareas y responsabilidades necesarias para implantar procedimientos que permitan resolver problemas y fallas.
- Lograr implantar y poner en marcha el plan de continuidad tecnológica en forma de prueba.
- Cada vez que se haga cualquier tipo de actualización sobre el sistemas actual de igual manera se replique en el sitio Off-Site, con el fin de estar alertas a cualquier situación presentada.
- Divulgar y crear la cultura entre los funcionarios de la Entidad para así saber con certeza que si se llegara a presentar cualquier eventualidad se tenga el norte de una actuar inmediato.
- Las entidades del gobierno deben integrar sus servicios con el fin que estos no salgan tan caros, existiendo un pacto de cooperación mutua entre ellas, con el propósito de fortalecer esfuerzos y poder prestar servios baratos entre entidades y además ser mas competidas frente a empresas del sector privadas, es necesarios crear alianzas de mutuo acuerdo.

CONCLUSIONES

Alertar a las directivas de la magnitud de las amenazas y riesgos a los que está expuesto el centro de cómputo de la UAEAC, los posibles desastres que se pueden presentar y formulando en la monografía las posibles alternativas de solución para de esta manera tomar las acciones previsivas antes de que ocurra un desastre.

Poner en funcionamiento los sistemas de información más críticos como son PAF, PISTA, ALDIA, MIGRAR, SIGMA e INTERNET, en un centro de cómputo alternativo escogido para no perder continuidad en las operaciones diarias de la Entidad en el cual necesita adicionalmente tener servidor INTERNET y SERVIDOR SERVICIOS DE RED.

Internet: No se tiene un control eficiente en portales ya que los usuarios de la Entidad deben acceder a Internet para buscar o publicar temas que tiene que ver con su trabajo, pero no se ha podido controlar el acceso a páginas porno y el software ilegal.

Correo electrónico: Los usuarios de la Entidad puede enviar y recibir indiscriminadamente correo de cualquier portal, esto ocasiona que se filtren virus que afectan la red y de igual manera es una herramienta de trabajo interno para las diferentes oficinas.

GLOSARIO

Incendios: Es uno de los fenómenos más frecuentes que se puede presentar en el mundo y no se puede descartar por completo a pesar de las medidas de seguridad que se tengan, siempre existirá un grado de riesgo.

Inundaciones: Este tipo de riesgo es considerado pero en caso de desastre natural ya que por características de infraestructura no se considera debido a que el centro de cómputo se encuentra ubicado en un sitio que no es susceptible de presentarse.

Terremoto: Se contempla este riesgo debido al alto riesgo al que se está expuesto por la posición geológica de la ciudad de Bogotá, ya que la capa tectónica se encuentra soportada por una losa de piedra que se extiende hasta la ciudad de Medellín, si se llega a presentar un terremoto lo más probable es que afecte considerablemente las dos ciudades.

Temblor: Se considera porque la posición geológica de la ciudad de Bogotá, hace que se este expuesto a este riesgo.

Actos de sabotaje y/o Terrorismo: El sector donde esta ubicado el Centro Nacional de Aeronavegación donde opera el centro de cómputo es un punto de alto riesgo para este tipo de actos.

Continuidad operativa: Que mediante la operatividad del hardware, software y los sistemas de información se garantice la operación normal de la U.A.E.A.C.

Red de información Avenida Eldorado (Calle 26) de la Ciudad de Bogota: esta avenida se ha convertido en uno de los sectores mas importantes para las comunicaciones en Bogotá ya que por ésta existe una gran infraestructura subterránea para el funcionamiento de las comunicaciones de diferentes empresas que están ubicadas en esa vía y que prestan servicios a gran parte del país y que por lo tanto han invertido sumas importantes para mantener operativo su negocio.

T.I.	Tecnología Informática
UAEAC	Unidad Administrativa Especial de Aeronautica Civil
PAF PISTA	Planeamiento Administrativo y Financiero Proyecto de Integración Sistemas de Transito Aéreo
ALDIA	A utomatización en L ínea D e I nformación A eronáutica
MIGRAR	Nombre del Servidor utilizado para hacer las migración de JDEdwards V.7334
SIGMA	Sistema de Información de Gestión de Mantenimiento de la Aeronautica Civil.
SAN	Storage areal Network(area de almacenamiento en red) es tecnología de punto y consiste en que el arreglo de discos en un servidor ya no se deja para que trabaje en el mismo rack donde reside la CPU, si no que esta en otro rack o área totalmente independiente y se comunica a la CPU a través de fibra óptica, su función es de tener un armario independiente de discos para mejor administración y fácilmente puede crecer en tamaño de acuerdo a las necesidades del usuario.
FAN	Fondo Aeronáutico Nacional
ERP	Enterprice Resources Planning, herramienta que se encarga de integrar diferentes sistemas de información, con el fin de optimizar la producción de una empresa.
LAN TO LAN	Enlace de comunicaciones que se establece entre dos redes LAN, para este documento el termino se utiliza para decir el enlace entre el centro de computo principal con el centro de computo definido como Off_Side.
Off_Side	Centro de computo alterno definido para planes de contingencia, cualquier solución que se adopte.
E1	Término utilizado para describir un ancho de banda de 2 Mg/Seg.

FO

Fibra óptica

Switch

Dispositivo utilizado en telecomunicaciones para recibir y entregar señales de datos.

ANEXOS

ANEXO 1. Estructura Orgánica de UNIDAD ADMINISTRATIVA ESPECIAL DE AERONAUTICA CIVIL

ANEXO 2 Sistemas de Información y su Relación con las Dependencia de la UAEAC

ANEXO 3 Sistema de Información y su Relación con la UAEAC.

ANEXO 4 Tabla Alternativa Centro de Computo

ANEXO 5 Sistemas de Información

ANEXO 6 Grafico Riesgo de Aplicativos

ANEXO 7 Matriz Riesgo de Aplicativos

ANEXO 8 Matriz Sistemas de Información

ANEXO 9 Identificación de Riesgos

ANEXO 10 Alternativa Centro de Computo alterno

ANEXO 11 Costo – Beneficio

ANEXO 12 Cronograma de Actividades

ANEXO 13 Control Ingreso de Personal

BIBLIOGRAFIA

Auditoria y Control Empresarial, Universidad Antonio Nariño, educación a distancia, 1994.

Información de Internet.

Documentación Dirección de informática de la U.A.E.C.

Documentación de la Entidad Unidad Administrativa Especial de Aeronáutica Civil.

Auditoria y Evaluación de Sistemas.

<http://www.sire.gov.co/websire/biblioteca/institucional.htm>

Planes de Contingencia TIC y continuidad del negocio
En colaboración con Upgrade, The European Journal for the Informatics Professional, revista digital promovida por CEPIS (Council of European Professional Informatics Societies).

Controles para la continuidad de negocio en ISO 17799 y COBIT 15
José Fernando Carvajal Vión, Miguel García Menéndez.