UNIVERSIDAD DE PANAMA
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO
FACULTAD DE INFORMATICA, ELECTRÓNICA Y COMUNICACIONES
UNIVERSIDAD CARLOS III DE MADRID

GUÍA PARA EL DESARROLLO DE UN PLAN DE RECUPERACION DE DESASTRES (DRP) PARA EL IFARHU, PANAMA

ERASMO CEDEÑO

ASESORES
DR BENJAMÍN RAMOS ALVAREZ
DRA ALMUDENA ALCAIDE

TÉSIS PRESENTADA COMO UNO DE LOS REQUISITOS PARA OPTAR AL GRADO DE MAESTRÍA EN GESTIÓN Y TECNOLOGÍA DEL CONOCIMIENTO

PANAMA, REPÚBLICA DE PANAMA
2013

18 MAR 2014

UNIVERSIDAD DE PANAMÁ
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO
DIRECCIÓN DE POSTGRADO

VIP-DP--12
17 de enero de 2013

Ingeniera
Amarilis De León
Coordinadora
Maestría en Gestión y Tecnología del Conocimiento
Facultad de Informática, Electrónica y Comunicación
Universidad de Panamá
E. S. D.

Estimada Señora Coordinadora:

Atendiendo su solicitud de inscripción del Proyecto de Intervención, adjunto copia de la misma con su respectivo código para los trámites pertinentes.

NOMBRE DEL ESTUDIANTE	TÍTULO DEL PROYECTO	CÓDIGO
José Guillermo	Evaluación del Entorno Organizacional para la Implementación de un Plan de Recuperación de Desastres de Tecnología en la AIG- Análisis de Impacto al Negocio.	CE-PI-327-17-03-13-01
Erasmo Cedeño	Guía para el Desarrollo de un Plan de Recuperación de Desastres (DRP) para el IFARHU, Panamá.	CE-PI-327-17-03-13-02
Roberto Chan NG	Guía para la Implantación de un Plan de Recuperación ante Desastres (DRP) para el IFARHU, Panamá	CE-PI-327-17-03-13-03
Gustavo Chery	Diseño de un BPM (Business Process Management) o Gestión de procesos de Negocios a través de un Bus de Servicio Empresarial SOA (Arquitectura Orientada	CE-PI-327-17-03-13-04
Lastenia Degracia Murillo	Estrategia de Inteligencia de Negocios.	CE-PI-327-17-03-13-05

CIUDAD UNIVERSITARIA OCTAVIO MÉNDEZ PEREIRA
Estafeta Universitaria, Panamá, República de Panamá
Tels.: (507) 523-5320 Fax: (507) 523-5310
Correo electrónico: upvipdp@ancon.up.ac.pa

Benilda Paz	Una VDI con enfoque de Inteligencia de negocio un caso práctico	CE PI 327 17-03-13-16
Maribel Wong	Eficiencia en los Municipios Panameños utilizando herramientas de Gobierno Electrónico	CE PI 327 17-03-13-17
Miguel Ángel Zelada M	Diseño de arquitectura orientada a servicio a través de un Bus de Servicio Empresarial	CE PI-327 17-03-13-18
Armando Zurita	Sistemas Inteligentes para la reducción del hacinamiento carcelario basado en la clasificación de privados de libertad mediante el uso de brazaletes y el desarrollo de la video audiencias	CE PI-327 17-03-13-19

Atentamente

Dr Filiberto Morales
Director de Postgrado

Adj lo indicado

/bed

UNIVERSIDAD DE PANAMÁ
VICERRECTORÍA DE INVESTIGACIÓN Y POSTGRADO

ACTA DE SUSTENTACIÓN
DEL PROYECTO DE INTERVENCIÓN

SEDE Facultad de Informática, Electrónica y Comunicación

PROGRAMA DE MAESTRÍA EN Gestión y Tecnología de del Conocimiento

Título del Proyecto de Intervención Guía para el desarrollo de un Plan de Recuperación de Desastres (DRP) para la IFARHU. Panamá.
Nombre del Participante CEDEÑO RIOS, ERASMO BIENVENIDO
Cédula 8-346-388
CIP Nº _____

Miembros del Jurado **Calificación otorgada**

NOMBRE Y FIRMA DE LOS MIEMBROS DEL JURADO		TRABAJO ESCRITO	DEFENSA	PROMEDIO
NOMBRE	FIRMA			
DR AGAPITO LEDEZMA		48	46	94
DR. ANGEL GARCIA OLAYA		48	45	93
DR IVAN ARMUELLES VOINOV		48	47	95
			NOTA FINAL	94

Recomendaciones del Jurado
Revisar ortografía del Documento final

Firma del Director de Investigación y Postgrado o Coordinador del Programa

Firma del Representante de la VIP

Firma del Estudiante

Fecha 28/1/13

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ABREVIATURAS

AIG: Autoridad para la Innovación Gubernamental.

ASE: Asesor de Seguridad.

BIA: por sus siglas en inglés: Business Impact Analysis, análisis de impacto del negocio.

BCI: sus siglas en inglés: Business Continuity Institute, Instituto de Continuidad del Negocio.

CDs: por sus siglas en inglés: Compact Disk: Disco Compacto utilizado para almacenar información.

COBIT: sus siglas en inglés: Control OBjectives for Information and Related Technology. Objetivos de Control para tecnología de la información y relacionada.

CIT: Coordinador de Infraestructura Tecnológica.

CRTI: Coordinador de Recuperación de TI.

DELL: DELL es una compañía multinacional estadounidense establecida en Round Rock (Texas) que desarrolla, fabrica, vende y da soporte a computadoras personales, servidores, switches de red, programas informáticos, periféricos y otros productos relacionados con la tecnología.

DRII: sus siglas en inglés: Disaster Recovery Institute International

DRP: sus siglas en inglés: Disaster Recovery Plan, Plan de Recuperación ante Desastres.

DS4: Dominio de Cobit. Delivery and Support.

IEEE: sus siglas en inglés: Institute of Electrical and Electronics Engineers.

IFARHU: Instituto para la Formación y Aprovechamiento de los Recursos Humanos.

ISO: sus siglas en inglés: International Organization for Standardization

ITIL (del ingles Information Technology Infrastructure Library) Biblioteca de Infraestructura de Tecnologias de Informacion es un conjunto de conceptos y practicas para la gestión de servicios de tecnologias de la información el desarrollo de tecnologias de la información y las operaciones relacionadas con la misma

MTD sus siglas en inglés Maximun Time Down Tiempo máximo tolerable fuera de servicio

NIST sus siglas en inglés National Institute of Standards and Technology que se traduce en Instituto Nacional de Estandares y Tecnologia

P09 Proceso de Cobit Evaluar y Administrar los riesgos de TI

RPO sus siglas en ingles Recovery Point Objective Punto de recuperacion objetivo

RTO sus siglas en inglés Recovery Time Objective tiempo de recuperación objetivo despues de un desastre

SAN en ingles (Storage Area Network) es una red de área de almacenamiento

SLA por sus siglas en ingles (Service Level Agreement) Acuerdo de Nivel de Servicios

OSI por sus siglas en ingles (Open System Interconnection) Interconeccion de sistemas abiertos

TI sus siglas en inglés Information Technology Tecnologia de la Información

TICs sus siglas en ingles Information Technology and Comunications Tecnologia de la Informacion y Comunicaciones

USB Universal Serial Bus Dispositivo de almacenamiento que utiliza una memoria flash para guardar información

UPS por sus siglas en ingles (Uninterruptible Power Supply) Fuente ininterrumpida de poder

WRT por sus siglas en ingles Work Recovery Time Tiempo de Trabajo de Recuperacion

RESUMEN

En este trabajo de fin de master realizaremos una Guía para el Desarrollo de un Plan de Recuperación de Desastres para el Instituto para la Formación y Aprovechamiento de los Recursos Humanos. Nos enfocaremos específicamente en los equipos considerados críticos para la institución en el desarrollo de esta guía. En primera instancia realizamos un resumen funcional y operativo de la institución con sus organigramas. Luego describimos la situación del ambiente informático del IFARHU, configuraciones y topologías. Definimos la metodología a utilizar en el desarrollo del plan, el alcance del mismo, identificamos los desastres probables o las amenazas más comunes en Panamá. Identificamos los equipos críticos del IFARHU, determinamos los requerimientos de operación para estos equipos críticos. Lo anterior nos permite desarrollar el Análisis de Impacto al Negocio (BIA) y de Riesgo. Todos estos componentes nos ayudaron a desarrollar esta guía, donde identificamos el recurso humano interno y externo requerido para la recuperación de desastres, el procedimiento para activar el plan, y el procedimiento general de recuperación para cualquiera de los equipos críticos de la institución. Además se desarrolla un procedimiento para devolver los sistemas al estado original una vez finalizada la contingencia y otro para evaluar y dar mantenimiento al plan de recuperación de desastres.

SUMMARY

In this final master work, we will carry out a Guide for Developing a Disaster Recovery Plan for the Instituto para la Formación y Aprovechamiento de los Recursos Humanos. We will focus specifically on equipment considered critical to the institution in developing this guide. In the first instance, we performed a functional and operational summary of the institution using their charts. Then, we described the situation of the environment of IFARHU, configurations and topologies. Define the methodology used in developing the plan, its scope and likely identify common disasters and threats in Panama. We identified the critical equipment of IFARHU and determined the operating requirements for these critical equipments. It will allow us to develop the Business Impact Analysis (BIA) and Risk. All these components helped us to develop this guide, where we identified the internal and external human resources required for disaster recovery, the procedure for activating the plan, and the overall recovery process for any of the critical equipment of the institution. Also, we develop a procedure to return the original state systems after the contingency and another to evaluate and maintain the disaster recovery plan.

INTRODUCCIÓN

Lo que significa un desastre dentro de una organización puede tener muchas definiciones. Es esta investigación procedimos a entrevistar varios directores de tecnología de diferentes instituciones gubernamentales donde les preguntamos que entendían por un desastre en sus áreas de trabajo y la mayoría concordó que para las instituciones gubernamentales un desastre puede ser desde la pérdida importante de datos hasta un desastre natural que deja inservible la infraestructura tecnológica. Por lo anterior descrito indicamos que cualquier evento que produzca una interrupción en las operaciones normales de un negocio o actividad es considerado un desastre. Lo anterior genera la necesidad de contar con un plan para la recuperación de desastres [1] para los sistemas y equipos críticos. Generalmente la mayoría de las organizaciones si no cuentan con este plan no se recuperan ante interrupciones generadas por fenómenos naturales, los cuales regularmente son los causantes de estos desastres.

El tema de los planes para darle continuidad a un negocio o actividad, realmente no es algo nuevo. A diario convivimos con estos, que se hace imperceptible su utilización. Sea cual fuese la medida que se utilice para afrontar un riesgo, las acciones están orientadas a buscar alguno de los siguientes objetivos: mitigar, evitar o transferir el riesgo identificado, y en algunas ocasiones hasta asumirlo.

A diario las personas practican las acciones de evitar, transferir o mitigar los riesgos. Algunos de los conceptos manejados en el ambiente de recuperación por desastre en primera instancia parecieran tener el mismo significado, sin embargo, cada área tiene

caracteristicas muy particulares Segun investigaciones realizadas existen tres grandes áreas en la que se debe ubicar la estrategia de una organizacion para administrar el riesgo inherente a su operatividad diaria, las indico a continuacion

Plan de Recuperación en caso de Desastre DRP por sus siglas en ingles (Disaster Recovery Planning) Son las acciones para recuperarse en caso de que se presente un desastre **Plan de Recuperación del Negocio** BRP por sus siglas en ingles (Business Recovery Planning) este lleva un paso más adelante del DRP ya que además de procesamiento de datos se enfoca en recuperar el resto de las operaciones de la empresa o institución y por ultimo el concepto de **Plan para Continuidad del Negocio** BCP por sus siglas en inglés (Business Continuity Planning) este ultimo le permite a la empresa, negocio o institucion su funcionamiento durante e inmediatamente se declare un desastre o emergencia[2]

El presente trabajo nos permitirá contar con una guia que nos ayude a desarrollar un procedimiento o plan de recuperación a seguir en caso de que se presente un desastre natural en el sistema informatico el mismo estará dirigido a los equipos criticos de manera que los servicios que se ofrezcan a través de estos equipos tecnológicos se puedan habilitar en un sitio alterno y que la institución continue su operación desde el otro lugar mientras se recupera el sitio original Por lo tanto el trabajo a realizar en este trabajo de fin de maestria tiene un enfoque para ser aplicado a una institucion gubernamental en Panamá, nos referimos especificamente del Instituto para la Formación y Aprovechamiento de Recursos Humanos (IFARHU)

El IFARHU es la institución gubernamental en Panamá que se encarga de ofrecer financiamiento y becas para estudios a nivel primario secundario universitario (Licenciaturas Carreras Tecnicas y de Postgrados) para la formación de profesionales En esta institucion se llevan una serie de servicios criticos soportados por una infraestructura tecnológica sobre la cual desarrollaremos el DRP Es por esta razón que la alta disponibilidad de estos sistemas se vuelve un asunto critico y la mejor forma de asegurar esta disponibilidad es contar con un procedimiento de manera proactiva que permita habilitar los sistemas en caso de un desastre haciendo que estos incidentes en los sistemas sean lo más transparente posible para sus usuarios permitiendo la continuidad de los servicios

Otra parte importante que se debe tomar en cuenta cuando se desarrolla este tipo de proyectos es el sitio alterno o lugar escogido para hospedar los equipos y sistemas que se van a utilizar como medida de contingencia es caso de desastre Estos sitios alternos varian desde una simple área cerca del centro de operaciones hasta el alquiler de centros especializados para estos tipos de actividades Estos ultimos cuentan con todas las facilidades en equipo infraestructura y seguridad sin embargo tienen un alto costo el cual se vuelve relativo cuando se habla de que puede ser la diferencia entre seguir o no ofreciendo los servicios Otros elementos no menos importantes que se deben tomar en cuenta en este tipo de desarrollo de planes son el contenido y redacción de los mismos o sea, sin ser expertos en los sistemas a habilitar y sin fuertes conocimientos tecnicos en informatica, pueda ser capaz de tomar el plan o procedimiento y activar los procesos en el

sitio alterno Razón por la cual a lo largo de esta investigacion para el desarrollo del DRP se hará énfasis en la calidad de la información contenida en el plan

Finalmente es importante mencionar que esta institución (IFARHU) cuenta con una gran cantidad de sistemas y equipos informáticos sin embargo esta investigación se concentrará en los equipos criticos y sistemas que soportan los principales servicios que se ofrecen a traves de la tecnologia

ESTADO DEL ARTE

En el estado del arte de este trabajo definiremos una breve descripción de cuál es el objetivo que se busca al desarrollar este proyecto, la metodología de trabajo a utilizar, el problema existente, la propuesta que desarrollaremos, un glosario de términos que iremos desarrollando en la medida que avance la investigación. Lo anterior sería lo que compone el estado del arte de este proyecto.

El objetivo de este proyecto es desarrollar una guía o Plan de Recuperación de Desastres para los equipos críticos del IFARHU, dar a conocer la guía para que personal del centro de cómputo y ajeno a este departamento pueda seguirla en un momento dado para ejecutar los procedimientos y poder darle continuidad a los servicios que se ofrecen a través del centro de cómputo, además dentro de la guía definiremos el procedimiento de mantenimiento de dicho plan de recuperación. Como anteriormente lo describimos el proyecto estará enfocado en dos trabajos que se presentarán por separados, uno orientado a los equipos críticos del centro de cómputo del IFARHU y el otro a los sistemas críticos (software).

Por ser dos trabajos separados existirá concordancia en varios componentes del proyecto, pero que al momento de la etapa de desarrollo del plan se evidenciará cuando se hable de equipos y cuando se haga de sistemas.

La metodología del trabajo que utilizaremos para desarrollar este documento en el cual crearemos la guía para el desarrollo del DRP del IFARHU la cual estará orientada a

los equipos considerados criticos para la institución comprenderá desde la parte inicial del proyecto y finalizara con la creacion del procedimiento que permita el mantenimiento del plan

La metodologia a utilizar para el desarrollo del plan contempla realizar lo siguiente

- **La conceptualización** del plan para los equipos criticos En esta etapa definiremos el alcance del plan los objetivos se identificará el recurso humano para el desarrollo del plan la administración del DRP se desarrollará el procedimiento para la aprobación del DRP y se identificarán los desastres probables en Panamá (amenazas naturales)
- **El Diseño del Plan,** contempla el desarrollo del inventario de los equipos y sistemas que conforman la plataforma tecnológica del IFARHU se identificaran los sistemas y equipos criticos se clasificarán los equipos segun su grado de criticidad se determinarán los requerimientos necesarios de procesamiento de los equipos y sistemas criticos
- **Respaldo de los sistemas y equipos criticos** que debe respaldarse y la frecuencia, los sitios alternos para la recuperación
- **Definiremos los procedimientos de implantación y control del DRP,** el cual incluye la puesta en marcha del plan la definicion de las pruebas y el procedimiento de mantenimiento del plan

Esta metodologia está basada en las recomendaciones del National Institute of Standards and Technology (NIST) Disaster Recovery Institute International (DRII) y el Business Continuity Institute (BCI) apoyandonos también en la habilidad conocimiento y experiencia del personal de Tecnologia del IFARHU en el manejo y operación de los

equipos y sistemas Otro aspecto considerado son investigaciones que realizaremos a través de la web literatura escrita (libros manuales) estandares COBIT 4 1 ISO (International Organization for Standarization) El dominio Delivery and Support (DS4) de COBIT lo he utilizado para apoyarnos a tener un adecuado enfoque para la continuidad de las operaciones Este dominio tiene como objetivo garantizar la continuidad del servicio Ademas hemos realizado entrevistas a personal clave de la institución

Un aspecto importante en el desarrollo de proyectos como este donde la investigación que se realice debe quedar bien referenciada y descrita en el proyecto dado esto utilizaremos el formato IEEE para el estilo y las referencias bibliográficas utilizadas en el desarrollo de esta investigación

Análisis de Impacto (BIA) y de Riesgo

El BIA se considera como uno de los principales componentes al momento del desarrollo de un DRP En él se busca determinar la variedad de hechos o imprevistos que pueden tener un efecto en la funcionalidad de los procesos de una institución o entidad
A continuación describiremos estas actividades

- Analizaremos el **impacto del negocio (BIA)** sobre el servicio de las tecnologias de información de los servicios criticos

  Determinaremos el **RTO RPO y MTD** de cada equipo o sistemas considerado critico los cuales definiremos o estimaremos a través de encuestas o entrevistas con el personal clave de la empresa que manejan y operan los sistemas con lo

anterior definiremos los procedimientos de recuperación que se utilizarían en el DRP

- **Se hará la identificación de riesgos,** desarrollaremos una matriz de riegos para los sistemas y equipos críticos del IFARHU y la probabilidad de ocurrencia de los desastres naturales
- Desarrollaremos que proteccion debemos tener en los centros de cómputo contra amenazas naturales
- Que seguridad física deben tener los sistemas críticos
- Analizaremos y definiremos el sitio alterno para los servicios críticos

Finalmente desarrollaremos el Plan en si donde definiremos el recurso humano requerido para el DRP los roles y responsabilidades del personal que participará Definiremos las contrataciones necesarias para el DRP de los sistemas y equipos críticos del IFARHU incluirá el desarrollo del procedimiento para darle mantenimiento al DRP

Como todo proyecto constara de unas conclusiones y recomendaciones así como de las referencias utilizadas para la investigación

PROPUESTA (OBJETIVOS Y MOTIVACIÓN)

El Instituto para la Formación y Aprovechamiento de los Recursos Humanos (IFARHU) es una institución gubernamental la cual tiene como fin el desarrollo de un proyecto o programa que permita garantizar el aprovechamiento apropiado y oportuno, formando técnicamente y utilizando racionalmente el recurso humano producido en el país como medio para que se acelere el desarrollo social y económico[1].[3]

Para lograr este objetivo el IFARHU se apoya en los equipos tecnológicos y sistemas que se encuentran en el centro de cómputo de la institución, los cuales son administrados por la Dirección de Tecnología Informática.

Uno de los aspectos que se deben considerar en la gestión administrativa y operativa de los centros de cómputos de instituciones gubernamentales en Panamá es la necesidad de planes de continuidad de operaciones en caso de que existan desastres naturales o factores internos que interrumpan los servicios que se ofrecen en los mismos. Lo anterior nos obliga al desarrollo de una guía o plan de recuperación ante desastres, que ayude a mitigar los riesgos productos de desastres naturales en Panamá y que afecten los servicios que se ofrecen a través de los equipos y sistemas críticos del centro de cómputo del IFARHU.

[1] Información obtenida de la página Web del IFARHU en la siguiente dirección: http://www.ifarhu.gob.pa/ifaweb/Historia3.aspx

Por lo tanto el objetivo general de este proyecto consiste en

Desarrollar una guia (Plan DRP) que le permita a la Dirección de Tecnologia Informática del IFARHU minimizar el tiempo de la interrupción el dano y el impacto asociado a los procesos criticos del negocio soportados por los servicios brindados por TI frente al escenario de contingencia

También contará con objetivos especificos

Contar con los procedimientos para recuperar los equipos criticos ante desastres naturales en un lugar alterno y en un tiempo determinado asi como tambien el procedimiento para devolver los equipos y sistemas criticos a su centro original cuando termine la contingencia

- Dar a conocer a los usuarios claves el contenido del Plan de Recuperación ante Desastres

Establecer el procedimiento para el mantenimiento del Plan de Recuperación ante Desastres

CAPÍTULO I. ANTECEDENTES.

1.1 ORIGEN DEL IFARHU.

En los años 60 la República de Panamá se encontraba en condiciones económicas no muy favorables, el gobierno de la época se formuló como una de sus metas eliminar la paralización económica existente en Panamá, creando una entidad que ayudara a resolver el problema del recurso humano en nuestro país, proporcionando el recurso humano capacitado para que contribuyera con el crecimiento de la economía. Producto de lo anterior se gestiona la creación de la Ley No. 1 de 11 de Enero de 1965, con la cual nace el Instituto para la Formación y Aprovechamiento de los Recursos Humanos (IFARHU)[3]

Los criterios fundamentales bajo la cual se crea esta institución se enuncian a continuación[2]:

1. Económico: para enfrentar el bajo desarrollo económico, se debía educar y capacitar a una nueva persona, con mentalidad renovada, que contribuya con este nuevo conocimiento al impulso de los sectores que conforman la economía nacional.
2. Educativo: reduciría la deserción escolar, producida por la difícil situación económica

[2] Información pública obtenida del Sitio Web del IFARHU en http://www.ifarhu.gob.pa/ifaweb/Historia1.aspx

que atravesaba el pais

3 Social existia mucha dificultad para crear y desarrollar proyectos que ayudaran el crecimiento de la economia y que estos no tuviesen relacion con la capacitación y formación de las personas

4 Politico teniamos que desprendernos de manera urgente ya que contábamos con mucha dependencia foránea o extranjera

En adición a los criterios enunciados anteriormente se indicaba que para que exista un equilibrio entre el desarrollo económico y social debia adherirse a las otras inversiones que se estaban dando en el pais una politica que permitiese formar y utilizar el recurso humano cuyo fin fuese identificar a esa población activa de manera económica capaz de atender las necesidades que el progreso y desarrollo reclaman

El IFARHU en este lapso estableció una estructura organizacional cuya especialidad fue formar e implementar un programas de becas préstamos y planificar la formación del recurso humano panameño

A finales de los años 60 se da un movimiento revolucionario en Panama, denominado la Revolución del 11 de Octubre de 1968 Luego de esto en el IFARHU se da una reorganización administrativa, tecnica y legal donde la caracteristica principal se enmarcó en buscar nuevos valores que permitieran el afianzamiento de los principios positivos con los que contaba el IFARHU y que permitieron la apertura de nuevas actividades

Posteriormente en los anos 70 la educación fue identificada como un elemento generador por excelencia de la transformacion económica y social

Con la formación del Seguro Educativo bajo el decreto de Gabinete No 168 del 27 de Julio de 1971 el IFARHU utiliza este impuesto para impulsar el desarrollo de nuevos programas que ayudan a mejorar el sector educativo panameno

Para esa época el IFARHU inicia la creación de tres nuevos centros estudiantiles distribuidos en tres provincias del pais (Cocle Chiriqui y Los Santos) con el fin de apoyar a la población estudiantil con alojamiento alimentacion y formación educativa, permitiendo que estudiantes de estratos sociales bajos y con difícil situación económica pudiesen educarse e integrarse al recurso humano capacitado que necesitaba el pais

Con la firma de los Tratados Torrijos Carter en el ano 1977 era necesario que el pais contara con un instrumento de formación y capacitación que ayudara a promover el acceso a mano de obra calificada panameña para reemplazar a la estadounidense cuando el Canal de Panamá pasase a ser administrado por los panamenos

Los anos 70 se caracterizaron como de democratizacion y expansion producto a al origen de los nuevos programas de *Becas Comunitarias el Programa de Perfeccionamiento a Servidores Publicos y Asistencia Educativa se incrementaron los montos del Programa de Credito Educativo y se promocionan los estudios y/o investigaciones tendientes a determinar las necesidades de formacion profesional y tecnica y la promocion de los recursos ya formados integrandolos a las actividades de produccion* [3]

[3] Información obtenida de la página web del IFARHU http //www ifarhu gob pa/ifaweb/Historia1 aspx

Lo anterior da origen a la creación del Departamento de Aprovechamiento de Recursos Humanos el cual tenia como objetivo dar mayor contenido a la filosofia humanistica institucional ya que permite llevar hasta la bolsa de trabajo a los ex beneficiarios ademas se crea del Centro de Documentacion Información y Orientación Educativa, a través de la Resolución No 820 de 20 de Noviembre de 1979

Para la década de los 80 se aumenta el otorgamiento de creditos educativos en todo el pais aumentando la promoción económica y social que ayudarian a mejorar el nivel de vida de los panameños Para esta decada nació el lema *Educar para el desarrollo* etapa esta que estuvo proyectada en términos de desarrollo y crecimiento Se conformaron programas básicos tales como la planificacion del recurso humano el crédito y la asistencia educativa la administración la finanza, la información y documentación

La mayoria de las becas y préstamos se destinaron para la gente con mucha humildad y de gran talento a nivel nacional

Luego se crean otros tres centros estudiantiles en las provincias de Coclé Darién y Veraguas donde se albergaban estudiantes y se les proveia de alimentos y alojamiento permitiéndoles que personas de estratos humildes y de lugares remotos pudiesen asistir a estos lugares a estudiar y formarse

A inicio de los 90 se agudiza una crisis económica en el pais ademas se crea una nueva administracion en la institución la cual realiza un estudio por dirección y departamentos que conforman el IFARHU a nivel nacional con la finalidad de conocer la situacion real de la institución y tomar medidas para afrontar la crisis económica

Esta etapa se define hasta el mes de agosto del ano 1994 donde se reactivan algunos programas que fueron utilizados con anterioridad y que habian quedado sin utilizar para tratar de alcanzar los niveles de servicios ofrecidos en los años ochenta

En el mes de septiembre de 1994 se da inicio a una etapa que se caracterizo por la activación el fortalecimiento y la ampliación de los programas habituales de crédito becas y asistencia educativa, aunado a lo anterior se crean nuevos programas de asistencia económica educativa para los hijos de las personas que murieron en diciembre 20 de 1989 cuando se da la invasión estadounidense a Panamá Se crean también otros programas de becas para los corregimientos más pobres del pais y para estudiantes con discapacidades

También se promueven compromisos internacionales otorgando becas y créditos para aumentar la poblacion estudiantil panamena en el exterior

Se crea una agresiva politica financiera con la finalidad aumentar los niveles de crédito educativo tambien se establece la creación de un juzgado ejecutor quien se encargaria de la recuperación de la morosidad existente de los prestamistas Además se diseña una campana de publicidad encaminada a dar a conocer los servicios que el IFARHU brinda a los ciudadanos panameños

La union de estas tres variables se utiliza para estructurar al IFARHU con la finalidad de obtener altos niveles de rendimiento eficiencia financiera y administrativa Además tres variables internas de la institución ayudaron a fortalecer los servicios que la institucion ofrecia, estas tres variables fueron

- Aplicacion de tecnologia en sus procesos internos

- Información y retroalimentación de la misma en todos los niveles de la organización, es decir entrenamiento en el uso de la tecnología.
- Optimización del potencial humano, dentro de la Institución.

Con estas variables se logra se logra potenciar la estructura organizacional del IFARHU, haciéndola muy eficiente en sus procesos internos y logrando altos rendimientos en sus operaciones.

En septiembre del año 1999, se inicia una nueva administración pública en el país, cuyo objetivo estaba encaminado a la modernización todos los servicios públicos, y cuya primacía o preferencia fue brindar respuestas a las clases más humildes y necesitadas del país, bajo el lema "*TRABAJAMOS JUNTOS POR PANAMÁ*".

Bajo este aspecto el IFARHU cumplía con todos los lineamientos señalados y se proyecta primeramente como una Institución de desarrollo e implementación en tecnología informática en el ámbito nacional, con la finalidad de equipar a todas sus oficinas a nivel nacional durante el año 2001, de tal manera tal que se brinden servicios de calidad a sus colaboradores y usuarios.

Para el 2002, se da una modificación en el Seguro Educativo mediante la Ley No.49 de 18 de septiembre, en la cual se disminuye el porcentaje correspondiente al IFARHU.

En esa administración y con el lema "*DESARROLLANDO EL TALENTO NUEVO DEL PAÍS*"[4], se da inicio al proceso que busca la modernización y fortalecimiento institucional, con lo cual se estable el Plan Estratégico 2005-2009, cuya finalidad

[4] Información obtenida de la página web del IFARHU en http://www.ifarhu.gob.pa/ifaweb/Historia3.aspx

consistia en [5] *Desarrollar un programa que garantice el adecuado aprovechamiento en la formacion tecnica y la utilizacion racional de los recursos humanos de la Republica como medio de acelerar su desarrollo economico y social* Este se basó en los cuatro pilares basicos

[6] *Planificacion de los Recursos Humanos*

- *Becas*
- *Asistencia Economica*

  Credito Educativo
- *Que ademas incluye el mejoramiento de la red de comunicacion en las diferentes sedes de la Institucion*

Entre el mes de septiembre del ano 2004 y el mes de diciembre del ano 2007 se otorgaron ciento ocho mil cuatrocientas nueve (108 409) becas por un monto de sesenta y dos millones doscientos veintiocho mil doscientos sesenta y ocho dolares con cuarenta y cinco centavos ($62 228 268 45) Se crearon nuevos programas tales como *el de Bellas Artes el de Formacion y Capacitacion del Talento Humano en Areas Prioritarias Asistencia Economica para la Erradicacion del Trabajo Infantil Pasantias para la Capacitacion de Profesionales Agropecuarios en Cultivos de Agro-exportacion Auxilio Economico Complementario Servidores Publicos y Docentes Universidades Oficiales Estudiantes de Escasos Recursos en el Exterior Pago de Matricula para Estudiantes de*

[5] Información obtenida de la página web del IFARHU en http //www ifarhu gob pa/ifaweb/Historia3 aspx
[6] El plan estratégico del IFARHU para los años 2005 al 2009 se basó es estos 4 pilares básicos Información obtenida de la página web del IFARHU

Universidades Oficiales tambien se creo el Programa de Becas Doctorales y Postdoctorales y el Programa de Excelencia Profesional a su vez se hace la reforma a la Ley Organica No 1 de 11 de enero de 1965 mediante Ley No 23 de 29 junio 2006 ademas se modifico el Reglamento de Becas Asistencia Economica y Auxilios Economicos [7] Con lo anterior se apoya a formar y aprovechar el recurso humano de acuerdo a lo establecido en el Objetivo Misión y Vision del IFARHU en esa época

En diciembre del ano 2004 se establece la jornada sobre Formación de Recursos Humanos con la cual se pretendia obtener información sobre estudios la oferta y demanda de formación de recursos humanos imprescindibles para el aumentar el desarrollo del pais al nivel de la educación media y superior

Luego en el año 2006 se da otra jornada de formación donde se buscó descubrir cuál era la verdadera demanda para formar los recursos humanos en las áreas de desarrollo

Tambien se conforma la Oficina de Cooperación Técnica Internacional mediante Resolución No 320 2006 369 de 28 de julio de 2006 además se establecen las Direcciones Provinciales Comarcales de Ngobe Bugle y de Emberá de Darien mediante Resolución No 320-2006 371 de 31 de julio de 2006

A la Oficina de la Mujer le cambian el nombre y pasó a llamarse Oficina de Igualdad de Oportunidades la cual es creada a traves de la Resolución No 320 2007 25 de 31 del 12 de enero de 2007

Con la resolución No 12 del 28 de diciembre de 2006 se actualiza el Reglamento de Credito A traves de este nuevo reglamento se formulan siete nuevos modelos de credito que buscan beneficiar a la población estudiantil además se da lugar a la creación de una

[7] Información obtenida de la página web del IFARHU

moratoria y condonación de deuda la cual se beneficiara a trece mil ochocientos sesenta y cinco (13 865) estudiantes prestatarios del pais

Con la modernizacion del IFARHU durante este periodo se concretaron alianzas con instituciones nacionales e internacionales se han firmado mas de treinta convenios de cooperación con diversas entidades e instituciones para que se le permita a los panamenos educarse entrenarse y desarrollar sus habilidades Esto se da a traves de convenios de cooperacion educativa y técnica, becas y préstamos para estudiar y entrenarse en universidades internacionales

1.1.1 OBJETIVOS DEL IFARHU.

[8] *"Objetivos Estratégicos de la Institución*

- *Planificar la formación y aprovechamiento del capital humano requerido para el desarrollo integral del país.*
- *Estimular a estudiantes y profesionales panameños de alto desempeño académico.*
- *Apoyar el desarrollo del talento nacional en las artes, el deporte y la cultura.*
- *Administrar efectivamente los recursos para las becas y auxilios educativos provenientes del Estado, personas naturales, entidades públicas y privadas en el nivel nacional e internacional.*
- *Manejar con equidad los fondos destinados por el Estado a la asistencia económica educativa a estudiantes que procedan de la población vulnerable y en situación de riesgo.*
- *Ofrecer crédito educativo para estudios de educación primaria, premedia, media y superior en las áreas demandadas para el desarrollo nacional.*
- *Desarrollar adecuadas políticas y estrategias de cobro que conduzcan a una recuperación eficiente y eficaz.*
- *Modernizar la institución mediante una simplificación administrativa expedita para ofrecer servicios eficientes y eficaces a los usuarios y clientes."*

---

[8] Esta es una información pública y definida por la alta dirección del IFARHU, la cual se obtuvo del siguiente sitio web http://www.ifarhu.gob.pa/ifaweb/misionvision.aspx

1.2 ORGANIZACIÓN DEL IFARHU POR DEPARTAMENTOS.

El Instituto para la Formación y Aprovechamiento de Recursos Humanos (IFARHU) cuenta con una estructura orgánica bien definida. La misma está compuesta de niveles los cuales describimos a continuación, además en cada uno de estos niveles se encuentran las áreas o direcciones que conforman cada "*nivel*[9].

- ***Nivel Político y Directivo***
  - *Consejo Nacional.*
  - *Dirección General.*
  - *Subdirección General.*
- ***Nivel Coordinador.***
  - *Secretaría General.*
- ***Asesoría Legal.***
  - *Oficina de Información y Relaciones Públicas.*
  - *Oficina de Igualdad de Oportunidades.*
  - *Oficina de Cooperación Técnica Internacional.*
- ***Nivel Fiscalizador.***
  - *Auditoría Interna.*
  - *Oficina de Control Fiscal de la Contraloría General de la República.*
- ***Nivel Auxiliar de Apoyo.***
  - *Dirección de Administración.*

---

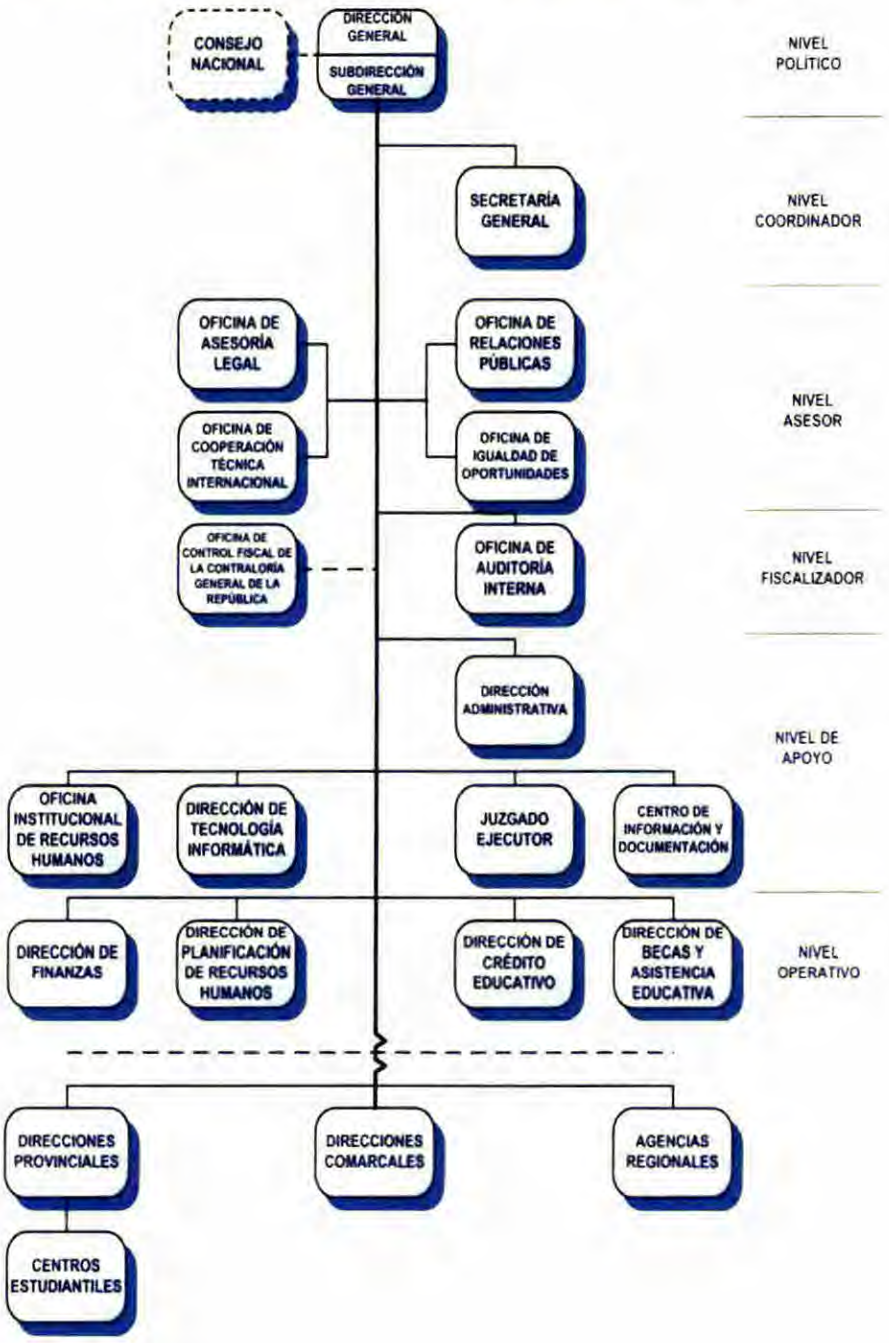
[9] Información pública obtenida del sitio web del IFARHU, http://www.ifarhu.gob.pa/ifaweb/Estructura.aspx

- *Oficina de Informatica*
- *Oficina Institucional de Recursos Humanos*
- *Juzgado Ejecutor*
- *Centro de Informacion y Documentacion*

- ***Nivel Operativo***
  - *Direccion de Planificacion*
  - *Direccion de Finanzas*
  - *Direccion de Credito Educativo*
  - *Direccion de Becas y Asistencia Educativa*
  - *Direcciones Provinciales*
  - *Direcciones Comarcales*
  - *Centros Estudiantiles*
  - *Agencias Regionales*

1.2.1 ORGANIGRAMA GENERAL.

Figura 1. Organigrama General del IFARHU Año 2012.



Como se observa en la Figura 1, el IFARHU cuenta con un organigrama bien definido en niveles y estos niveles compuestos por direcciones, áreas y oficinas que apoyan la gestión que la institución realiza. Estas divisiones bien marcadas en el organigrama facilitarán el desarrollo y aplicación del plan de recuperación de desastres.

1.2.2 ORGANIGRAMA DE LA DIRECCIÓN DE TECNOLOGÍA INFORMÁTICA Y SUS FUNCIONES.

Figura 2. Organigrama de la Dirección de Tecnología Informática.

Dirección de Tecnología Informática.

Objetivos

1. [10]*"Planificar, dirigir, organizar, coordinar y supervisar la automatización de los procesos, adquisición y mantenimiento de las tecnologías de información y comunicaciones utilizadas por el Instituto para la Formación y Aprovechamiento de Recursos Humanos a nivel nacional, en apoyo a las directrices emanadas del Despacho Superior y garantizando altos estándares de seguridad en su funcionamiento. "*
2. Implementar lo concerniente a planes de mantenimiento preventivo y correctivo de los recursos informáticos de la institución, velando por que se cumplan los procedimientos y estándares recomendables, apoyándose en el personal interno y/o contratos externos con empresas especializadas" [5].

Las funciones[11] de la Dirección de Tecnología Informática del IFARHU se encuentran en el Manual de Organización y Funciones del IFARHU, documento público confeccionado por el Departamento de Desarrollo Institucional del IFARHU.

---

[10] El Objetivo de la Dirección de Tecnología del IFARHU se encuentra definido en el Manual de Organización y Funciones del IFARHU el cual se encuentra disponible en: http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf

[11] Funciones de la Dirección de Tecnología Informática del IFARHU las podemos encontrar en el Manual de Organización y Funciones del IFARHU en el siguiente acceso web: http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf
Páginas 39, 40 y 41

Para conocer las funciones de la Dirección de Tecnología Informática del IFARHU pueden acceder al siguiente enlace, en las páginas 39, 40 y 41 del documento antes mencionado:

http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf

Consideramos no describir las funciones de ninguno de los departamentos de la Dirección de Tecnología Informática en este documento ya que como lo indiqué anteriormente son de carácter público y las mismas se encuentran avaladas por la Dirección Superior de la Institución

Subdirección de Tecnología Informática.

Objetivo

> [12] *"Colaborar con la Dirección de Tecnología de Información y Comunicación en la gestión de los procesos de automatización, adquisición y mantenimiento de las tecnologías de información y comunicaciones utilizadas por el Instituto para la Formación y Aprovechamiento de Recursos Humanos a nivel nacional."*

Funciones

Las funciones de la Subdirección [13] de Tecnología Informática del IFARHU se encuentran descritas en el documento Manual de Organización y Funciones del IFARHU en el siguiente acceso web http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf en las páginas 41 y 42.

---

[12] El Objetivo de la Subdirección de Tecnología del IFARHU se encuentra definido en el Manual de Organización y Funciones del IFARHU el cual se encuentra disponible en: http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf En la página 41 del Documento.

[13] Las funciones de la Subdirección se encuentran en un documento público y fueron desarrolladas por el Departamento de Desarrollo Institucional del IFARHU.

Departamento de Desarrollo de Sistemas

Objetivo

[14] *"Diseñar, implementar y administrar los Sistemas de Información Tecnológica utilizados por el Instituto para la Formación y Aprovechamiento de Recursos Humanos y todas sus dependencias a nivel nacional, en apoyo a las directrices emanadas de la Dirección de Tecnología Informática."*

Funciones

Las funciones del Departamento de Desarrollo de Sistemas[15] de la Dirección de Tecnología Informática del IFARHU se encuentran descritas en el documento Manual de Organización y Funciones del IFARHU en el siguiente acceso web, en la página 43.

http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf

[14] El Objetivo del Departamento de Desarrollo de Sistemas de la Dirección de Tecnología Informática del IFARHU se encuentra definido en el Manual de Organización y Funciones del IFARHU el cual se encuentra disponible en: http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf en la página 43.

[15] Las funciones del Departamento de Desarrollo de Sistemas de la Dirección de la Dirección de Tecnología Informática del IFARHU se encuentran en un documento público y fueron desarrolladas por el Departamento de Desarrollo Institucional del IFARHU.

Departamento de Soporte Técnico

Objetivo

[16]*"Diseñar y supervisar los programas de mantenimiento preventivo y correctivo de los equipos computacionales y periféricos que hacen posible el funcionamiento de los Sistemas de Información Tecnológica utilizados por el Instituto para la Formación y Aprovechamiento de Recursos Humanos y todas sus dependencias a nivel nacional."*

Funciones

Las funciones del Departamento de Soporte Técnico[17] de la Dirección de Tecnología Informática del IFARHU se encuentran descritas en el documento Manual de Organización y Funciones del IFARHU en el siguiente acceso web, en la página 44.

http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf

Departamento de Telecomunicaciones

Objetivo

[18]*"Diseñar, implementar y administrar de los Sistemas de Telecomunicaciones de Voz, Imágenes, Internet y Datos que hacen posible el funcionamiento de los Sistemas de Información Tecnológica utilizados por el Instituto para la Formación y*

---

[16] El Objetivo del Departamento de Soporte Técnico se encuentra definido en el Manual de Organización y Funciones del IFARHU disponible en la web, documento PDF en: http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf en la página 44.

[17] Las funciones del Departamento de Soporte técnico de la Dirección de Tecnología Informática del IFARHU se encuentran en un documento público y fueron desarrolladas por el Departamento de Desarrollo Institucional del IFARHU.

Aprovechamiento de Recursos Humanos y todas sus dependencias a nivel nacional."

Funciones

Las funciones del Departamento de Telecomunicaciones [19] de la Dirección de Tecnología Informática del IFARHU se encuentran descritas en el documento Manual de Organización y Funciones del IFARHU en el siguiente acceso web, en la página 45.

http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf

Departamento de Procesamiento de Datos

Objetivo

[20] *"Diseñar, implementar, administrar el mantenimiento de la base de datos en los Sistemas de Información Tecnológica utilizados por el Instituto para la Formación y Aprovechamiento de Recursos Humanos y todas sus Dependencias a nivel nacional, en apoyo a las directrices emanadas de la Dirección de Tecnología Informática."*

---

[18] El Objetivo del Departamento de Telecomunicaciones del IFARHU las encontramos definidas en el Manual de Organización y Funciones del IFARHU disponible en la web, documento PDF en: http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf
En la página 45 del documento.

[19] Las funciones del Departamento de Telecomunicaciones de la Dirección de Tecnología Informática del IFARHU se encuentran en un documento público y fueron desarrolladas por el Departamento de Desarrollo Institucional del IFARHU.

[20] El Objetivo del Departamento de Procesamiento de Datos de la Dirección de Tecnología Informática del IFARHU las encontramos definidas en el Manual de Organización y Funciones del IFARHU disponible en la web, documento PDF en: http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf
En la página 46 del documento.

Funciones

Las funciones del Departamento de Procesamiento de Datos[21] de la Dirección de Tecnología Informática del IFARHU se encuentran descritas en el documento Manual de Organización y Funciones del IFARHU en el siguiente acceso web, en la página 46. http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf

[21] Las funciones del Departamento de Procesamiento de Datos de la Dirección de Tecnología Informática del IFARHU se encuentran en un documento público y fueron desarrolladas por el Departamento de Desarrollo Institucional del IFARHU.

1.3 SITUACIÓN ACTUAL DEL AMBIENTE INFORMÁTICO DEL IFARHU.

El IFARHU por ser una institución gubernamental, creada desde el 11 de Enero de 1965 [5], está orientada a la formación del recurso humano especializado, otorgándoles becas y financiamiento para estudios, cuenta con una estructura y ambiente tecnológico que le permite a la institución apoyarse en estos, para lograr las metas y objetivos establecidos permitiéndoles ejecutar las operaciones de una forma eficaz y continua.

La gestión de Tecnología en las instituciones gubernamentales en Panamá se encuentra supervisada por la Autoridad Nacional Para Innovación Gubernamental (AIG) quien es la entidad responsable de la modernización del Estado, mediante el uso de las Tecnologías de Información y Comunicaciones (TICs). Todos los proyectos de adquisición de equipos y software de las instituciones gubernamentales deben contar con el aval de la AIG, inclusive nos guían y orientan en la formulación de proyectos tecnológicos. Descrito lo anterior todo proyecto relacionado con la tecnología de las instituciones debe tener el aval de la AIG.[6]

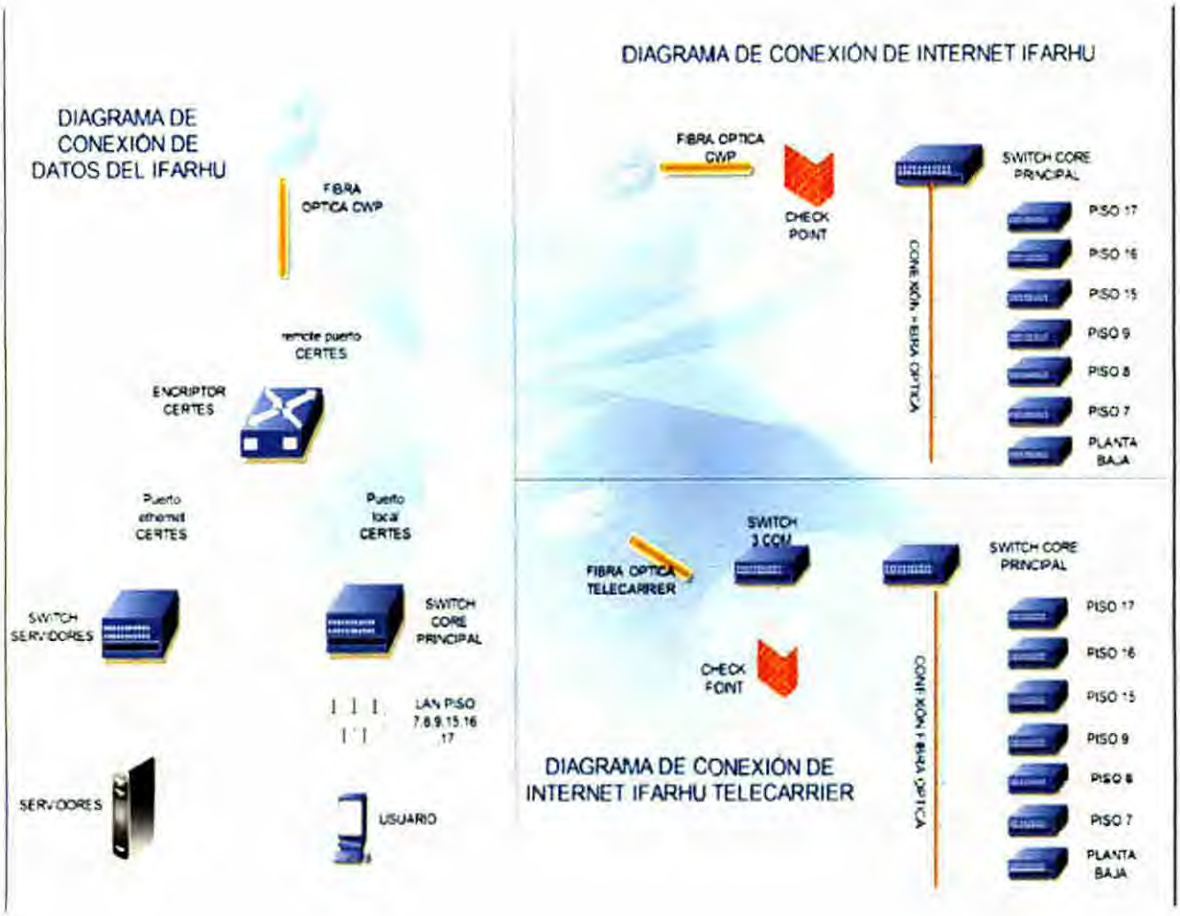
1.3.1 CONFIGURACIONES Y TOPOLOGÍAS.

La fortaleza de la operación del IFARHU está ligada al nivel tecnológico que se encuentra desarrollado en la institución, por ese motivo tener una buena configuración de los equipos y una topología de red adecuada es fundamental para ofrecer un buen soporte a los usuarios de nuestros sistemas. Cuando hablamos de topología nos referimos a la ruta por la que discurren los datos a través de la red. Hay tres tipos básicos de topologías: de

bus de estrella y de anillo En una topologia de bus cada estación de trabajo y el servidor estan conectados a través de un cable central llamado bus En una de red de anillo el cableado va de estación en estacion sin que haya un principio ni un final En una red de estrella todas las estaciones de trabajo están conectadas al servidor pero no entre ellas

La red de área local (LAN) del IFARHU cuenta con una topologia de estrella, conectando los pisos del edificio a través de una fibra óptica con un Switch Core principal a los switches de los diferentes pisos En la Figura 3 encontraran los diagramas de conexión de los datos internos y conexiones de internet del IFARHU

Figura 3. Diagramas de conexiones de la Red del IFARHU del Centro de Cómputo ubicado en su sede principal, Avenida Ramón Arias, Edificio IFARHU, Piso 15.



CAPÍTULO II. METODOLOGÍA A UTILIZAR PARA EL DESARROLLO DEL PLAN DE RECUPERACIÓN DE DESASTRES.

2.1 CONCEPTUALIZACIÓN DEL PLAN DE RECUPERACIÓN DE DESASTRES PARA LOS SERVICIOS TECNOLÓGICOS CRÍTICOS DEL IFARHU.

En esta fase de la metodología para el desarrollo del plan de recuperación de desastres para los equipos tecnológicos críticos del Instituto para la Formación y Aprovechamiento de Recursos Humanos (IFARHU) se establecen las bases conceptuales y el planeamiento inicial sobre la cual se desarrolla este trabajo, la coordinación e inducción de los elementos que participen en el desarrollo del plan.

Dentro de la conceptualización realizaremos lo siguiente:

- Definiremos los objetivos.
- Se identificará el recurso humano para desarrollar el Plan de Recuperación ante Desastres (DRP).
- Se definirá el procedimiento para la aprobación del plan.
- Se desarrollará el procedimiento para identificar los desastres probables.

2.1.1 DEFINIR EL ALCANCE DEL PLAN DE RECUPERACIÓN DE DESASTRES (DRP) ANTE AMENAZAS NATURALES.

El alcance de este DRP establece que la Dirección de Tecnología Informática del IFARHU cuente con un documento o guía para restablecer las operaciones de TI y por ende de la institución, ante eventos que pudieran interrumpir la habilidad de lograr sus objetivos estratégicos, es un elemento clave para las organizaciones de todo tipo, y en especial la nuestra.

Los riesgos asociados son muy altos y la alta dependencia en las tecnologías de información y de telecomunicaciones ha motivado la necesidad de las organizaciones de contar con las medidas preventivas adecuadas y con la capacidad para recuperar la habilidad de entregar productos y servicios en el tiempo adecuado.

Cuando se desarrollan planes de recuperación de desastres debemos tener en cuenta el alcance del mismo, para lo cual procedemos a definir cuál sería el que utilizaremos en este DRP.

Esta Guía para el desarrollo del DRP del IFARHU comprenderá sólo los equipos considerados críticos, cuyas interrupciones sean ocasionadas por fenómenos naturales con miras a mantener la disponibilidad de los servicios críticos de la institución.

2.1.2 DEFINIR LOS OBJETIVOS DEL PLAN.

La planeación de un programa de recuperación de desastres es de gran importancia para las instituciones como el IFARHU, ya que al identificar los objetivos del mismo, nos permite desarrollar con eficiencia el contenido del DRP.

Un plan de recuperación de desastres (DRP), es el plan que ejecuta Tecnologías de la Información para recuperar los sistemas que gestiona [8]. Por lo tanto el mismo debe contar con un objetivo general y objetivos específicos que complementen el objetivo general. El plan de recuperación ante desastres, vendría a ser aquella parte del plan de contingencia y del plan de continuidad de negocios (BCP), que aborda aquellas contingencias que, por su gravedad, no permiten continuar la prestación de los servicios desde el centro local y debe continuarse el servicio desde un nuevo sitio. El DRP debe contemplar la vuelta atrás cuando tras arreglar las consecuencias del desastre, el servicio pueda ser reanudado en el sitio original [9]. Descrito lo anterior procedemos a definir el objetivo general y los objetivos específicos para el desarrollo del DRP del IFARHU.

En la **Tabla 1** que se muestra a continuación se describen los objetivos generales y específicos que fueron definidos para el desarrollo del DRP.

Tabla 1. Objetivos Generales y Especificos para el desarrollo del DRP de los equipos críticos del IFARHU.

TIPO DE OBJETIVO	DESCRIPCION DEL OBJETIVO
General	1. Desarrollar una guía (Plan DRP) que le permita a la Dirección de Tecnología Informática del IFARHU minimizar el tiempo de la interrupción, el daño y el impacto asociado a los procesos críticos del negocio soportados por los servicios brindados por TI, frente al escenario de contingencia.
Específicos	1. Contar con los procedimientos para recuperar los equipos críticos ante desastres naturales, en un lugar alterno y en un tiempo determinado, así como también el procedimiento para devolver los equipos críticos a su centro original cuando termine la contingencia. 2. Dar a conocer a los usuarios claves el contenido del Plan de Recuperación

	ante Desastres. 3. Establecer políticas o procedimientos para el mantenimiento del Plan de Recuperación ante Desastres.

2.1.3 IDENTIFICACIÓN DEL RECURSO HUMANO PARA EL DESARROLLO DEL DRP.

El desarrollo del DRP para los equipos que soportan los servicios críticos del IFARHU se puede realizar a través de consultores externos o desarrollarlo internamente por el personal de la Dirección de Tecnología Informática (Departamentos de Soporte, Redes y el Director y Subdirector de Tecnología) y asesorado por un Asesor en Seguridad Informática. Ambas opciones tienen ventajas y desventajas que se resumen en la **Tabla 2**.

Tabla 2. Ventajas y desventajas para el desarrollo del DRP internamente o a través de contratación externa.

RECURSO HUMANO	VENTAJAS	DESVENTAJAS
CONSULTORES EXTERNOS	- Equipo dedicado para el desarrollo.	- Alto costo del desarrollo del DRP.

	Conocimiento especializado en el tema y facilita el desarrollo Al ser externos a la institución observan con mayor facilidad nuevos requerimientos Generalmente en el desarrollo estos incluyen el mantenimiento del plan	Dependencia de los consultores externos para actualizar el plan
PERSONAL INTERNO DE LA DIRECCIÓN DE TECNOLOGÍA INFORMATICA Y ASESOR EN SEGURIDAD INFORMATICA	Acceso rápido y completo a la informacion Facilidad para realizar el inventario de equipos y su clasificación Conoce todas las medidas de seguridad implantadas Identificar con más	Poca experiencia en este tipo de desarrollo No es tiempo completo y el proyecto puede durar más tiempo No retención de personal clave para mantenimiento del plan

	facilidad los grupos de trabajo para conformar equipos de DRP. - No requiere altos costos para el desarrollo del DRP - El conocimiento se queda internamente en la institución.	

Visto lo descrito en la Tabla 2, decidimos realizar el DRP internamente, ya que hacerlo con consultores externos es muy costoso para la institución.

2.1.4 ADMINISTRACIÓN DEL PLAN DE RECUPERACIÓN DE DESASTRES.

Para poder realizar la administración del plan de manera ordenada y designar responsabilidades especificas se define el siguiente equipo de administración:

Figura 4. Diagrama del equipo administración del DRP

Coordinador de Administración

Tiene asignado las siguientes responsabilidades:

1. Encargado de supervisar y dar a apoyo al desarrollo de las distintas tareas ejecutadas por los comités que conforman al equipo de administración.
2. Supervisar y colaborar en la ejecución del Plan de Distribución.

Comité de Distribución

Tiene asignado las siguientes responsabilidades:

1 Garantizar la difusión del plan entre los miembros del equipo y mantener vigente el Plan de Distribución

2 Asegurar que los miembros del equipo de recuperación de desastres siempre dispongan de como mínimo dos copias actualizadas del plan una de las cuales debe mantenerse en el lugar del trabajo siendo las demas almacenadas en algun otro lugar seguro externo al IFARHU

Comité de Entrenamiento

Tiene asignado las siguientes responsabilidades

1 Velar por la definición y cumplimiento oportuno del Plan de Entrenamiento y Capacitación de los procedimientos de recuperación

2 Efectuar la planificación de los entrenamientos y asimismo notificar a los participantes e instructores acerca de los cronogramas y alcance de las pruebas establecidas

Comité de Pruebas

Tiene asignado las siguientes responsabilidades

1 Supervisar y dar apoyo durante la ejecución de las pruebas garantizando la ejecución de las mismas en los tiempos planeados

2 Registrar los resultados de las pruebas y participar activamente en las pruebas

3. Apoyar al personal de las líneas de negocio involucradas en la ejecución de las pruebas.

Comité de Mantenimiento

Tiene asignado las siguientes responsabilidades:

1. Contar con un conjunto de procedimientos de mantenimiento debidamente formalizados y documentados.
2. Revisar y analizar los impactos producidos por cualquiera de los cambios en los ambientes informáticos sobre el Plan de Recuperación de Desastres y proceder a su actualización.
3. Debe existir una coordinación entre el Comité de Distribución y Comité de Pruebas para la actualización de sus respectivos procedimientos, de manera que tengan en cuentan los cambios realizados al Plan de Recuperación de Desastres.

2.1.5 DESARROLLO DEL PROCEDIMIENTO PARA LA APROBACIÓN DEL DRP.

Finalizado el desarrollo del documento denominado Plan de Recuperación de Desastres para los equipos críticos que soportan los servicios esenciales del IFARHU, se debe crear un procedimiento para la aprobación del mismo.

Para que la creación de un DRP sea efectiva en instituciones gubernamentales como la nuestra, debemos conformar comités que apoyen la administración del plan asignándole responsabilidades a cada una de estos comites dentro de las cuales estaria la creación del procedimiento para la aprobación del plan DRP

Para esto debemos seguir los siguientes pasos o procedimientos

1 Un representante de Cada Comité en conjunto con la Auditoria Interna y el Asesor en Seguridad informática deben evaluar el documento creado por la Dirección de Tecnologia Informática

2 Luego de la evaluación y si están de acuerdo con el contenido se deben realizar las pruebas al DRP

3 Una vez realizada estas pruebas y si las mismas son satisfactorias el Comité de Pruebas en conjunto con la Auditoria Interna deben redactar una nota a la Dirección General del IFARHU indicando la satisfacción del Documento denominado Plan de Recuperación de Desastres para los equipos criticos

4 Luego la Dirección General del IFARHU emite un documento donde avala el DRP y solicita a la Dirección de Planificación[22] incorpore el documento al manual de Politicas y Procedimientos de la Institución

[22] Generalmente las instituciones Gubernamentales en Panamá tienen en su organigrama una Dirección de Desarrollo Institucional o de Planificación quienes tienen como una de sus funciones la publicación de Politicas y Procedimientos internos aprobados por la alta dirección

2.1.6 IDENTIFICAR DESASTRES PROBABLES (AMENAZAS NATURALES EN PANAMÁ).

Entendemos por amenazas naturales aquellos elementos del medio ambiente que son peligrosos para el hombre, causados por fuerzas extrañas a él. Para efectos de desastre, la amenaza se refiere a todos los fenómenos atmosféricos, hidrológicos, geológicos (volcánicos y sísmicos), y a los incendios por su ubicación, severidad, y frecuencia que tienen el potencial de afectar adversamente al ser humano, sus estructuras y actividades.

A continuación en la Tabla 3 describiremos las amenazas naturales más comunes, agrupadas por categoría física:

Tabla 3. Amenazas naturales más comunes, agrupadas por categoría

Características Físicas	Amenazas
Amenazas con características hidrológicas:	1. Inundaciones. 2. Desertificación. 3. Sequía. 4. Erosión y sedimentación. 5. Desbordamientos de ríos. 6. Inundaciones en edificios causadas por rupturas de tuberías,

	filtraciones por lluvia
Amenazas con características atmosféricas	1 Granizo 2 Huracanes 3 Tornados 4 Tormentas tropicales 5 Descargas eléctricas causadas por rayos
Amenazas con características Sísmicos	1 Fallas geológicas 2 Terremotos 3 Tsunamis
Amenazas con características Volcánicas	1 Ceniza 2 Gases 3 Flujo de lava
Amenazas con caracteristicas incendios	1 Matorrales 2 Bosques 3 Sabanas 4 Incendios en edificios

Segun informes y cronologias de desastres ocurridos en Panamá desde el ano 1990 hasta el 2002[10] se dan por inundaciones y tormentas tropicales que producen descargas eléctricas que afectan equipos tecnológicos Además para el ano 2011 las tormentas tropicales y las inundaciones tuvieron mayor porcentaje de ocurrencia en América, segun

fuente Disaster data A Balanced Perspective Issuen N°26 Diciembre 2011[11] Con lo anterior nos lleva a pensar que estas amenazas naturales (tormentas tropicales e inundaciones) serian las que pudiesen afectar el centro de cómputo del IFARHU sin embargo en los capitulos posteriores investigaremos más con el personal de tecnologia de la institución y con el Sistema Nacional de Protección Civil de Panamá para obtener sus experiencias y vivencias con los desastres naturales que pueden afectar la ciudad capital de Panamá y por ende el centro de cómputo del IFARHU ademas investigaremos en instituciones como ETESA (Empresa de Transmisión Electrica, S A) quienes llevan estadisticas de fenómenos hidrometeorológicos en el pais

2.2 DISEÑO DEL PLAN DE RECUPERACIÓN DE DESASTRE PARA LOS SISTEMAS CRÍTICOS DEL IFARHU.

Esta sección viene a ser una de las principales para el del desarrollo del DRP, ya que en esta realizaremos el inventario de equipos y programas que se les aplicará el plan de recuperación. Además identificaremos de ese inventario los equipos críticos, los cuales describiremos más adelante donde los Directores y Jefes de áreas del IFARHU a través de encuestas identifiquen los sistemas de información críticos para luego poder determinar los equipos críticos donde se encuentran instalados estos sistemas; en este desarrollo del DRP tomaremos en cuenta una de las principales actividades en los centros de cómputo, los respaldos.

2.2.1 DESARROLLO DEL INVENTARIO DE LOS EQUIPOS Y ENLACES DE COMUNICACIONES QUE CONFORMAN LA PLATAFORMA TECNOLÓGICA DEL IFARHU.

El inventario de equipos de cómputo del IFARHU, lo hemos realizado y lo describimos en dos categorías, la Tabla 4 identifica el inventario de Servidores, la Tabla 5 muestra los equipos y enlaces de comunicación.

Tabla 4. Inventario de Servidores del IFARHU

	Inventarios de Equipos del Centro de Cómputo del IFARHU (Servidores y Almacenamiento)					
	MARCA	**MODELO**	**PROCESADOR**	**DISCO DURO**	**MEMORIA**	**FUNCIÓN**
1	DELL	Modular Chasis PE 1855				Chasis
2	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	No está en uso
3	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	Servidor de Correo Electrónico B2 ***
4	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (RED HAT 4) APLICACIONES B3 ***
5	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (Red Hat 4) Base de datos Oracle B4 ***
6	DELL	POWEREDGE 1855	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	Linux (Vmware esx 3) B5 Servidor de Pruebas (STORAGE 1)
7	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B6 Aplicativo de cajas Bienes patrimoniales
8	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes ***
9	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes *** IfARHU-SIETE, IFARHU-GSI (STOREAGE 1)
10	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) Msa de Ayuda B8

						Contenido if-antivirus-01, ifarhu-seis, if-soporte-01, if-sysaid-01, server-printer, servidor printer HP, ssa-if01 (STORAGE 3)
11	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	WS 2008 R2 SERVIDOR DE SEGURIDAD (ANTIVIRUS) B9
12	DELL	EMC AX 150		6 X 750 GB		STORAGE 1 (1.5T) *** STORAGE 2 (2.0 T) STORAGE 3 (1.0 T)
13	DELL	EMC AX 4-5		12 X 1 TB		PROYECTO IFASIS *** Sistema de Planilla
14	DELL	POWEREDGE 860	INTEL PEMTIUM 2 X 2 (2.8 GHz)	2 X 500 GB	1 GB	WS 2003 R2 (ACTIVE DIRECTORY 1) ***
15	DELL	POWEREDGE 2850	INTEL XEON 2 X(3.40 GHz)	4 X 146 GB	4 GB	ws 2003 SERVIDOR WEB (FEDORA 5)
16	DELL	POWEREDGE 2950	INTEL XEON 4 X (2.0 GHz)	4 X 146 GB	2 GB	WS 2008 R2 servidor DHCP ***
17	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 APLICACIONES (WEB)- PROGRAMACION

						*** Intranet
18	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 BASE DE DATOS (SQL)- PROGRAMACION ***

Tabla 5. Inventario de equipos de Comunicaciones del IFARHU.

Inventario de Equipos de Comunicación del IFARHU				
	MARCA	**MODELO**	**CANTIDAD**	**FUNCIÓN**
1	EXTEME NETWORKS	SUMMIT X460 -24p	3	Switch de piso
2	EXTEME NETWORKS	SUMMIT X460 -48p	2	Switch de piso
3	EXTEME NETWORKS	SUMMIT X450a -24p	1	Switch de piso
4	CISCO	2800	1	Router
5	3COM	4500	1	Switch
6	MOTOROLLA	RFS 4000	1	Wireless en los pisos
7	CHECK POINT	UTM -1 3070	1	Firewall
8	CERTES	CEP-10 VSE	1	Encripta información entre la sede y las regionales

2.2.2 IDENTIFICAR LOS EQUIPOS CRÍTICOS.

Dado el alto nivel de importancia de las funciones y operaciones críticas del IFARHU que son apoyadas por la infraestructura tecnológica descrita en las Tablas 4 y 5 mostradas anteriormente, se ha procedido a escoger de estos inventarios los equipos (servidores y

equipos de comunicación) que se consideran críticos para la institución. Esta escogencia la hemos realizado en base a dos aspectos:

1. Identificando los Servicios Críticos para la institución y en cuales equipos se encuentran instalados.
2. De acuerdo a la función que ejercen estos equipos en el centro de cómputo.

A continuación los servidores y equipos críticos identificados:

Tabla 6. Inventario de equipos Críticos del Centro de Cómputo del IFARHU.

Inventarios de Equipos Críticos del Centro de Cómputo del IFARHU						
N°	**MARCA**	**MODELO**	**PROCESADOR**	**DISCO DURO**	**MEMORIA**	**FUNCIÓN**
1	DELL	Modular Chasis PE 1855				Chasis
2	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	Servidor de Correo Electrónico B2
3	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (RED HAT 4) APLICACIONES B3
4	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (Red Hat 4) Base de datos Oracle B4
5	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes
6	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes IFARHU-SIETE, IFARHU-GSI (STOREAGE 1)
7	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	WS 2008 R2 SERVIDOR DE SEGURIDAD

						(ANTIVIRUS) B9
8	DELL	EMC AX 150		6 X 750 GB		STORAGE 1 (1.5 T) STORAGE 2 (2.0 T) STORAGE 3 (1.0 T)
9	DELL	EMC AX 4-5		12 X 1 TB		PROYECTO IFASIS Sistema de Planilla
10	DELL	POWEREDGE 860	INTEL PEMTIUM 2 X 2 (2.8 GHz)	2 X 500 GB	1 GB	WS 2003 R2 (ACTIVE DIRECTORY 1)
11	DELL	POWEREDGE 2950	INTEL XEON 4 X (2.0 GHz)	4 X 146 GB	2 GB	WS 2008 R2 Servidor DHCP
12	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 APLICACIONES (WEB)-PROGRAMACION Intranet
13	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 BASE DE DATOS (SQL)-PROGRAMACION

2.2.2.1 CLASIFICACIÓN DE LOS EQUIPOS SEGÚN SU GRADO DE CRITICIDAD.

Luego de identificar los equipos críticos para el centro de cómputo del IFARHU, los clasificaremos según la siguiente escala:

Sistema Crítico Alto: un equipo para el centro de cómputo es considerado como Crítico Alto cuando una interrupción en uno de ellos causa la paralización de las operaciones que realiza el IFARHU a través de este equipo y el arreglo o remediación del mismo puede durar desde uno o varios días. Lo cual trae consigo un alto costo para las operaciones que se efectúan en la institución.

Sistema Crítico Medio: es considerado crítico medio cuando la interrupción de uno de estos equipos es de manera rápida y el mismo no tiene una gran incidencia en las operaciones que se realicen a través de este equipo. Su recuperación dura entre 4 a 8 horas.

Sistema Crítico Bajo: es considerado critico bajo cuando su interrupción afecta de manera mínima la operatividad del IFARHU, su recuperación y arreglo dura menos de 4 horas.

2.2.2.2 DETERMINAR LOS REQUERIMIENTOS NECESARIOS DE LOS SISTEMAS CRÍTICOS.

En este punto se procede a identificar cuáles son los requerimientos en cuanto a software y hardware que se necesitan para arrancar con el diseño del DRP de contingencia de los equipos críticos.

1. Copia de los CD's de instalación de cada uno de los equipos y sistemas críticos.
2. Manual, instructivo o procedimiento digital o impreso de la instalación y configuración de cada equipo y sistema critico.
3. CD's de los Sistemas Operativos de cada equipo crítico.

4. Respaldo completo de cada uno de los equipos y sistemas críticos.
5. Respaldo de las bases de datos de los sistemas críticos, actualizada al último día hábil.
6. Manual y procedimiento de restauración de esas bases de datos.
7. Contratos de Soporte vigentes de los sistemas y equipos críticos, con niveles de servicios acordes al grado de criticidad de cada equipo.
8. Personal de tecnología y funcional para que prueben los equipos y sistemas cuando se configuren en el sitio alterno.
9. Contar con las pruebas a realizar para los equipos y sistemas.
10. Contar la descripción de los resultados esperados de estas pruebas.

2.2.3 RESPALDO DE LOS EQUIPOS CRÍTICOS.

Conocidos los recursos necesarios para que los equipos críticos se mantengan en operación o se reduzca el tiempo de interrupción de estos cuando ocurran contingencias en los mismos, debemos asegurarnos de tener respaldos de estos.

De manera genérica necesitamos reguardar o respaldar:

- Los equipos críticos con características idénticas a los de producción en el sitio alterno.
    - Respaldo de las configuraciones (en digital e impresas)
    - Manuales de instalación y configuración.

- Procedimientos de instalación y configuración.

- Materiales o la proveeduría necesaria para poder ser utilizados en caso de emergencia. (Cintas, papel, tóner, cartuchos de tinta, CDs, etc.)

- Un centro de cómputo alterno (secundario) para realizar las mismas operaciones que se efectúan en primario. Esta instalación debe contener las necesidades básicas para poder realizar el trabajo y brindar el servicio que se da en el centro de cómputo primario.

- Una copia del documento Plan de Recuperación de Desastres del IFARHU en el centro de cómputo alterno para ser utilizado en caso de una contingencia.

Esta es una de las etapas más importantes para el diseño del plan de contingencia, ya que de nada vale tener un excelente plan de recuperación de desastres, con el diseño más adecuado, el personal mejor entrenado, si no contamos con la información bien resguardada, el lugar donde poder ubicarla y utilizarla ante una contingencia. Además COBIT 4.1 PO7.5 Dependencias sobre individuos [12], que conozca cómo aplicar el DRP en caso de no localizar el personal clave[23].

2.2.3.1 DEFINIR LO QUE DEBE RESPALDARSE Y LA FRECUENCIA.

Para definir lo que debe respaldarse y la regularidad con que se haga, se necesita saber exactamente cual información es la que se va a usar en el caso de una emergencia. Es

[23] PO 7.5 Dependence on individuals. Using COBIT 4.1 to Guide the Adoption and Implementation of Open Source Software obtenida en http://www.isaca.org/Journal/Past-Issues/2008/Volume-3/Documents/jpdf0803-using-cobiT-4.1.pdf. Página 4.

obvio que todos los archivos y programas de los sistemas criticos deben ser respaldados Estos respaldos deben incluir

Respaldos de software y documentación

Respaldos de aplicaciones y documentacion

Respaldos de bases de datos

Respaldos de las configuraciones de los equipos criticos

Materiales que sean necesarios para que los usuarios de los sistemas criticos y el personal de cómputo pueda trabajar

Copias del plan de DRP

Copias de los procedimientos de instalación y proceso de los sistemas criticos

En cuanto a la frecuencia que se deben realizar los respaldos podemos describir las siguientes

Cuando se adquiera un nuevo paquete de software o se instale una nueva versión de los sistemas operativos de los sistemas criticos También deben resguardarse una copia de los manuales

Cada vez que se actualicen los datos de las bases de datos

Cada vez que se modifique algun programa o se instale una nueva aplicacion

Cada vez que se modifique el DRP se deben obtener las copias necesarias para ser distribuidas con el personal clave para la ejecucion del mismo

- Cada vez que se actualice el inventario de equipos críticos se debe guardar la copia más actualizada.
- Cuando se incluya un nuevo material o se modifique los existentes para el procesamiento de los sistemas críticos.

2.2.3.2 SITIOS ALTERNOS PARA RECUPERACIÓN DE LOS EQUIPOS CRÍTICOS.

Instituciones como el IFARHU donde el servicio que se le brinde a los clientes es vital para mantener el negocio, nos hace llevar a tener sitios alternos de respaldo para que en momentos de contingencias extremas podamos dirigirnos a esos lugares y poder ofrecer el servicio que el centro de cómputo brinda a sus usuarios.

Este lugar debe tener características muy similares o mejores a las que actualmente se encuentran el centro de cómputo. En nuestro caso existen dos alternativas que deben ser evaluadas, la primera de ellas es tener una empresa que se dedique a realizar este tipo de proceso y que nos proveen los equipos críticos para realizar el respaldo; la otra es adquirir o alquilar un local para que el personal de tecnología instale los equipos y sistemas contingentes en este sitio. En este último caso se deben preparar las instalaciones en forma similar o mejor al sitio principal.

Se considera que la primera es la más factible, ya que el uso de esta empresa no nos daría problema al momento de utilizar sus instalaciones dado que se haría un contrato con esta, para procesar cuando se requiera, además son centros especializados de hospedajes

de equipos y de sistemas de misión crítica, en cambio la otra alternativa, además de instalar y configurar los equipos y las aplicaciones existirían costos de mantenimiento de aires acondicionados electricidad controles de humedad control contra incendios controles de seguridad de acceso etc que se tendrían que adquirir y administrar por parte del personal de la Dirección de Tecnología del IFARHU

2.3 DESCRIPCIÓN DEL PROCEDIMIENTO DE IMPLANTACIÓN Y CONTROL DEL DRP.

Posterior al desarrollo del plan de Recuperación de Desastres del IFARHU, es necesario que el mismo sea implantado, para lo cual debemos llevar a cabo una serie de pasos.

- ✓ Hacer un listado de personas a las que se le entregará copias del plan de contingencia (parcial o total).
- ✓ Este plan debe contener un directorio telefónico que incluya:
  - o Todos los miembros del Departamento de Tecnología del IFARHU responsables de asistir a implantar el plan en caso de un desastre.
  - o El Coordinador del Plan.
  - o Comité de Mantenimiento del Plan.
  - o Comité de pruebas del plan.
  - o Auditor de Sistemas.
  - o Asesor en seguridad Informática.
- ✓ Teléfonos de los responsables del centro de cómputo alterno de respaldo.
- ✓ Proveedores de equipos y sistemas críticos.
- ✓ Teléfonos de emergencia (Cruz Roja , Bomberos, Policía Nacional)
- ✓ Tener una lista de los materiales que se necesitan para la implementación del plan de Recuperación de Desastres.
- ✓ Tener definido y probado los procedimientos para arrancar los sistemas en el sitio alterno.

Luego de realizados los pasos anteriores, para asegurarse de que el plan tenga los resultados esperados para los cuales fue desarrollado el mismo debe ser probado. Esta prueba no está en el alcance de este proyecto, sin embargo posteriormente definiremos los pasos para realizar esta prueba.

2.3.1 PUESTA EN MARCHA DEL DRP.

El plan de Contingencia debe ponerse en funcionamiento una vez ocurra un fenómeno natural que afecten el o los equipos y sistemas críticos del centro de cómputo del IFARHU.

Dentro de las etapas o procesos que se deben considerar para poner en marcha el plan de recuperación de desastres tenemos:

a) El Director o el Subdirector de Tecnología e Informática del IFARHU debe informar al equipo administrador del DRP descrito en el punto 2.1.4 de este documento, el percance ocurrido.

b) El equipo Administrador del DRP en conjunto con personal de Tecnología evalúan el daño.

c) El equipo Administrador informa a la alta gerencia del percance.

d) Se pide autorización a la alta Gerencia para poner en práctica el DRP

e) Se informa al personal encargado de ejecutar el DRP para que el mismo se ponga en ejecución.

2.3.2 PRUEBAS DEL DRP.

Es un punto dentro del Plan de Recuperación de Desastres de gran consideración porque de nada vale tener un DRP escrito si el mismo no ha sido probado. Como anteriormente lo he indicado las pruebas al DRP no están incluidas en el alcance de este proyecto, sin embargo describiremos unas consideraciones a tomar en cuenta para cuando estas se realicen. Al ejecutar las pruebas, se pueden identificar aspectos que pueden ser mejorados dentro del plan de contingencia, también es una forma de revisar lo siguiente:

- Los procedimientos de recuperación.
- Que existan todos los materiales que se requieran.
- Los respaldos de software, datos y equipos son los adecuados y que los mismos estén actualizados.
- El entrenamiento del personal sea el apropiado.
- El sitio de respaldo externo sea adecuado y cumpla con las necesidades para procesar los sistemas y equipos críticos.

Las pruebas sirven de entrenamiento al personal que ejecutará el DRP cuando esto se requiera. Como propósito primordial las pruebas nos ayudan a identificar posibles deficiencias en los procedimientos que forman parte del plan.

Es recomendable realizar al menos una prueba anual del DRP en el sitio alterno de respaldo. Esta nos ayuda a evaluar la eficiencia del plan y a revelar sus carencias, para así corregirlas.

Existen ciertos requerimientos que se necesitan para la efectividad de las pruebas:

- Se debe establecer el escenario de la prueba.

- Se deben definir los objetivos de la prueba.
- Se deben identificar los resultados esperados en las pruebas.
- Documentar lo anteriormente descrito.
- Documentar los resultados.
- Hacer partícipe de las pruebas a la auditoría del IFARHU, para que valide los resultados obtenidos.

2.3.3 MANTENIMIENTO DEL DRP.

Todo Plan de Recuperación de Desastres requiere de mantenimiento continúo, ya que los procesos varían según pasa el tiempo y se anexan nuevos software o equipos que en ocasiones se hacen críticos para la institución. Si el plan no se actualiza, el mismo no podrá ser utilizado de manera efectiva durante una emergencia. Una de las formas de identificar que el DRP requiere ser actualizado, es cuando al mismo se le realizan pruebas.

Al plan de Recuperación de Desastre le debe dar mantenimiento cada vez que:

- ✓ Cambien o aumenten los sistemas o aplicaciones.
- ✓ Cambien o se adquieran nuevos equipos.
- ✓ Cambie o se actualice el sitio de respaldo externo.
- ✓ Cuando se modifiquen los procedimientos y los procesos internos.

Una de las funciones del Comité de Mantenimiento del Plan de Recuperación de Desastres es revisar que el plan esté actualizado, esto se logra calendarizando las fechas de revisión del DRP.

Otro aspecto importante es la distribución de la documentación del DRP cada vez que se actualice debe distribuirse De esta manera el Comité de Distribución del DRP mantiene distribuida la ultima versión del Plan de Recuperación de Desastres del IFARHU

CAPÍTULO III. ANÁLISIS DE IMPACTO (BIA) Y DE RIESGOS.

3.1 ANÁLISIS DE IMPACTO CUALITATIVO SOBRE LOS SERVICIOS DE LAS TECNOLOGÍAS DE INFORMACIÓN DE LOS SISTEMAS CRÍTICOS.

Para identificar las áreas que tendrían interrupciones de servicios que afecten el funcionamiento de la institución producto de desastres, realizaremos el Análisis de Impacto del Negocio (BIA)[13] de estos servicios.

Esta parte del proyecto estará orientada a los equipos críticos dado que existe otro proyecto del DRP que abarcará los sistemas y aplicaciones críticas.

En este análisis identificaremos los equipos críticos y estimaremos los tiempos que la institución toleraría en caso de un desastre.

El BIA es considerado un aspecto de gran importancia a tener en cuenta para desarrollar cualquier DRP. En el BIA se identifica los más importantes eventos que pueden tener una incidencia en la continuidad de los servicios que se ofrecen a través de estos equipos y sistemas. En este estudio nos centraremos en identificar dos de las amenazas naturales descritas en la Tabla 3, las más comunes en nuestro país o las que se han materializado en los últimos 10 años. Además evaluaremos como estas han afectado a los sistemas y equipos críticos de los centros de cómputo.

Según ITIL V3 Fundations dentro de la Gestión de la Continuidad de los Servicios de TI existe una meta principal y varios objetivos.

Meta consiste en soportar el proceso de Gestión de continuidad del Negocio asegurando que tanto los componentes del servicio como los tecnicos (computadoras sistemas redes aplicaciones datos y centros de cómputo) pueden ser recuperados dentro de los tiempos requeridos y acordados con el negocio o institución

Objetivos principales de Continuidad de Servicios de TI segun ITIL V3 Fundations

- Crear y actualizar el conjunto de planes de Continuidad de Servicios de TI y planes de recuperación de TI que soportan los Planes de Continuidad del Negocio (BCP) de la institución u organización
- Llevar a cabo ejercicios de Análisis de Impacto al Negocio (BIA) en forma periódica, con lo cual aseguramos que todos estos planes se mantienen alineados con los impactos y requerimientos del negocio los cuales están en cambios constantes
- Realizar constantemente la evaluación y gestión de riesgos para que estos no excedan a los acordados con el negocio y en nuestro caso con la institución

Para el Analisis de Impacto sobre los servicios del Negocio realizaremos una serie de actividades las cuales describo a continuacion

1 Identificación de los sitios fisicos validamos el listado de los lugares donde se encuentran los equipos criticos del IFARHU

2 Determinar cuales son los sistemas utilizados en el IFARHU

3 Se evalua cual es el nivel o grado critico de cada sistema Esta evaluación es realizada por personal de la institucion (Directores y Jefes de Departamento de las areas de servicio

de la institución). Al contar con la evaluación de criticidad de los servicios identificamos los equipos críticos del centro de cómputo del IFARHU.

4. Determinaremos el RTO, RPO y MTD [14] de cada sistema crítico: esto lo haremos mediante encuestas o entrevistas al personal clave que maneja operativamente los procesos o servicios que se ofrecen en la institución. Una vez conocidos los sistemas de información críticos y los equipos críticos del IFARHU, encontraremos el tiempo de recuperación objetivo (RTO) en inglés (Recovery Time Objective), el punto de recuperación objetivo (RPO), en inglés (Recovery Point Objective) y el MTD, en inglés (Maximun Time Down) o tiempo máximo tolerable que el servicio estaría fuera de operación, para cada equipo crítico en el centro de cómputo del IFARHU con la finalidad de definir cuáles serían los procedimientos para recuperación de estos equipos.

3.1.1 IDENTIFICACIÓN DE LOS SITIOS FÍSICOS

El IFARHU sólo cuenta con un solo sitio físico o centro de cómputo. Se encuentra ubicado en el Piso 15 del edificio IFARHU ubicado en Avenida Ramón Arias.

3.1.2 IDENTIFICAR SISTEMAS DE INFORMACIÓN QUE SE UTILIZAN EN LA INSTITUCIÓN.

Esta información es suministrada por la Dirección de Tecnología en entrevista realizada al Director del área. La pregunta que se hizo fue la siguiente:

Indicarnos el o los nombres de los sistemas de información que se encuentran alojados en el centro de cómputo de la institución. En la tabla 7 que se muestra a continuación se

identifican los sistemas de información del IFARHU indicados por la Dirección de Tecnología.

Tabla 7. Sistemas de información utilizados en el IFARHU.

Nombre del Sistema	Descripción
Sistema de Crédito	Solicitudes, trámites, desembolso y recuperación de los préstamos educativos
Sistema de Correo Electrónico	Sistema de correo interno, además es utilizado para contactar a los prestatarios y becarios.
Sistema de emisión de Planillas y Cheques	Utilizado para la generación de cheques para el pago a los estudiantes.
Sistema de Becas	Otorgamiento, trámites y seguimiento de becas
Sistema de digitalización de expedientes de crédito	Digitalización de expedientes de crédito

3.1.3 EVALUACIÓN DE LA CRITICIDAD DE LOS SISTEMAS DE INFORMACIÓN.

Esta evaluación es realizada a través de una encuesta por medio de entrevistas a cada uno de los funcionarios (Directores y Jefes de Departamento), fueron 15 personas indagadas donde se les leyó los sistemas de información utilizados en el IFARHU y le

solicitamos nos indiquen el nivel de criticidad que ellos consideran de cada uno de estos sistemas de información.

Para definir los niveles de criticidad nos basamos en los indicados en el punto 2.2.2.1 Clasificación de los equipos según su grado de criticidad (Crítico alto, Crítico Medio y Crítico bajo). Sólo le agregamos a esta evaluación el No Crítico, en donde su interrupción no afecta la continuidad del servicio y se les explicó a cada uno de los entrevistados estos niveles.

Tabla 8. Ejemplo de una encuesta para determinar los niveles de criticidad de los sistemas críticos.

Nombre del Sistema de Información	*Descripción*	*Crítico Alto*	*Crítico Medio*	*Crítico Bajo*	*No Crítico*
Sistema de Crédito	Solicitudes, trámites, desembolso y recuperación de los préstamos educativos	X			
Sistema de emisión de Planillas y Cheques	Utilizado para la generación de cheques para el pago a los estudiantes.		X		
Sistema de Correo	Sistema de correo	X			

Electrónico	interno, además es utilizado para contactar a los prestatarios y becarios.				
Sistema de becas	Otorgamiento, trámites y seguimiento de becas		X		
Sistema de digitalización de expedientes de crédito	Digitalización de expedientes de crédito			X	

Luego de terminada estas encuestas se procede a extraer la información de las mismas donde los resultados fueron los siguientes, que mostramos en la Tabla 9.

Tabla 9. Compendio de las encuestas de los sistemas de información críticos del IFARHU.

Nombre del Sistema de Información	*Descripción*	*Critico Alto*	*Critico Medio*	*Critico Bajo*	*No Critico*
Sistema de Crédito	Solicitudes,	12	3		

	trámites desembolso y recuperación de los prestamos educativos				
Sistema de emisión de Planillas y Cheques	Utilizado para la generacion de cheques para el pago a los estudiantes	2	12	1	
Sistema de Correo Electrónico	Sistema de correo interno además es utilizado para contactar a los prestatarios y becarios	10	3	1	1
Sistema de becas	Otorgamiento tramites y seguimiento de becas		10	3	2
Sistema de digitalización de	Digitalización de expedientes de		3	9	3

expedientes de crédito	crédito				

Analizando el compendio de las encuestas de criticidad indicadas en la Tabla 9 podemos definir el orden de mayor a menor de los sistemas informáticos del IFARHU de la siguiente manera (1 es de mayor criticidad y el 6 es el de menor)

1. Directorio Activo
2. Sistema de Crédito.
3. Sistema de Correo electrónico.
4. Sistema de emisión de Planillas y cheques.
5. Sistema de becas.
6. Sistema de digitalización de expedientes.

Al contar con el orden de criticidad de los sistemas de información podemos identificar los equipos críticos y el orden de criticidad de estos. Lo anterior es producto de que si ya tenemos cuales son los sistemas críticos buscamos en la Tabla 6 de los equipos críticos del IFARHU e identificamos que equipos soportan estos sistemas, los cuales describimos a continuación en la Tabla 10.

Tabla 10. Equipos críticos que soportan los sistemas de información críticos.

N°	MARCA	MODELO	PROCESADOR	DISCO DURO	MEMORIA	FUNCIÓN
	DELL	Modular Chasis PE 1855				Chasis
1	DELL	POWEREDGE 860	INTEL	2 X 500 GB	1 GB	

			PEMTIUM 2 X 2 (2.8 GHz)			WS 2003 R2 (ACTIVE DIRECTORY 1)
1	DELL	POWEREDGE 2950	INTEL XEON 4 X (2.0 GHz)	4 X 146 GB	2 GB	WS 2008 R2 servidor DHCP
6	DELL	EMC AX 150		6 X 750 GB		STORAGE 1 (1.5 T) STORAGE 2 (2.0 T) STORAGE 3 (1.0 T)
2	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (RED HAT 4) APLICACIONES B3
2	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	IFASIS (Red Hat 4) Base de datos Oracle B4
3	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	Servidor de Correo Electrónico B2
4	DELL	EMC AX 4-5		12 X 1 TB		PROYECTO IFASIS Sistema de Planilla
5	HP	PROLIANT DL-580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 APLICACIONES

						(WEB)- PROGRAMACION Intranet
5	HP	PROLIANT DL- 580 G5	INTEL XEON 4 X 6 CORE (2.4GHz)	8 x 72	32 GB	WS 2008 BASE DE DATOS (SQL)- PROGRAMACION
6	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes
6	DELL	POWEREDGE 1955	INTEL XEON 2 X 4 (3.00 GHz)	2 X 73 GB	4 GB	LINUX (Vmware esx 3) B7 Imágenes IfARHU-SIETE, IFARHU-GSI (STOREAGE 1)

En la Tabla 10 observamos una numeración de equipos que corresponden a los que soportan a los sistemas de información críticos. Observamos que existen 3 equipos con el número 5, estos identificados con este número, son los que soportan el sistema de información con criticidad 5 (Sistema de digitalización de expedientes), los equipos identificados con el número 1 son los que soportan el sistema de información

denominado Sistema de Crédito, el cual es el considerado el más crítico para la institución.

3.1.4 LOS TIEMPOS RTO, RPO Y MTD PARA LOS EQUIPOS CRÍTICOS DEL IFARHU.

Primeramente según el Instituto Nacional de Estándares de Tecnología (por sus siglas en inglés NIST, National Institute of Standards and Technology), los tiempos RTO, RPO y MTD, son considerados parámetros cuya relación íntima con la recuperación ante desastres se convierten en fuentes fundamentales para el desarrollo e implementación del plan en forma exitosa.

El RTO (Recovery Time Objective) no es más que el tiempo objetivo de recuperación, dicho de otra manera, cuánto puede permanecer la institución (IFARHU) sin la ejecución de una actividad o servicio que utilice una aplicación o un equipo de cómputo. Generalmente el RTO se asocia con el tiempo máximo de inactividad. Este tiempo es utilizado para definir con que periodicidad se realizarían los respaldos o backups de las configuraciones o información que contienen los sistemas; además es utilizado para definir los requerimientos de infraestructura que ayudarán al reinicio operacional de la actividad afectada, el cual pudiese ser un lugar alterno con características muy parecidas al que se encuentra en una empresa o institución. También pueden ser equipos alojados en otro sitio esperando para restaurarle la información respaldada, etc.

Si en las encuestas que realicemos para determinar este tiempo hay un RTO cuya mayoría de los encuestados indiquen que el valor es casi cero el IFARHU tendría que

adquirir equipos contingentes redundantes con replicación de datos en línea Ahora, si el resultado arroja que se debe contar con un RTO de 8 12 16 28 o superior bastaria con tener respaldada la informacion en los medios magnéticos que utiliza la institución para tal fin y esto seria suficiente para cualquier sistema de información critica en particular

El Punto Objetivo de Recuperación (RPO) representa el punto en el tiempo antes de una interrupción o falla del sistema, para que la misión / negocio datos de proceso se puede recuperar (dada la copia de seguridad más reciente de los datos) después de un desastre o interrupción A diferencia de RTO el RPO no es considerado como parte de la MTD Más bien es un factor de la cantidad de pérdida de datos que el sistema de información puede tolerar durante el proceso de recuperación El RPO nos debe indicar la cantidad de información que puede la institución perder Dicho de otra manera, si el IFARHU efectua sus resguardos o backups todas las noches a las 10 00 p m y se presenta una interrupción al siguiente dia a la 1 00 p m toda información que se introdujo en el sistema desde la hora que se realizó el backup hasta el momento en que se presente la interrupción se perderia, dada a que la misma no se encuentra resguardada en el respaldo Entonces el RPO seria el respaldo efectuado la ultima noche antes del desastre

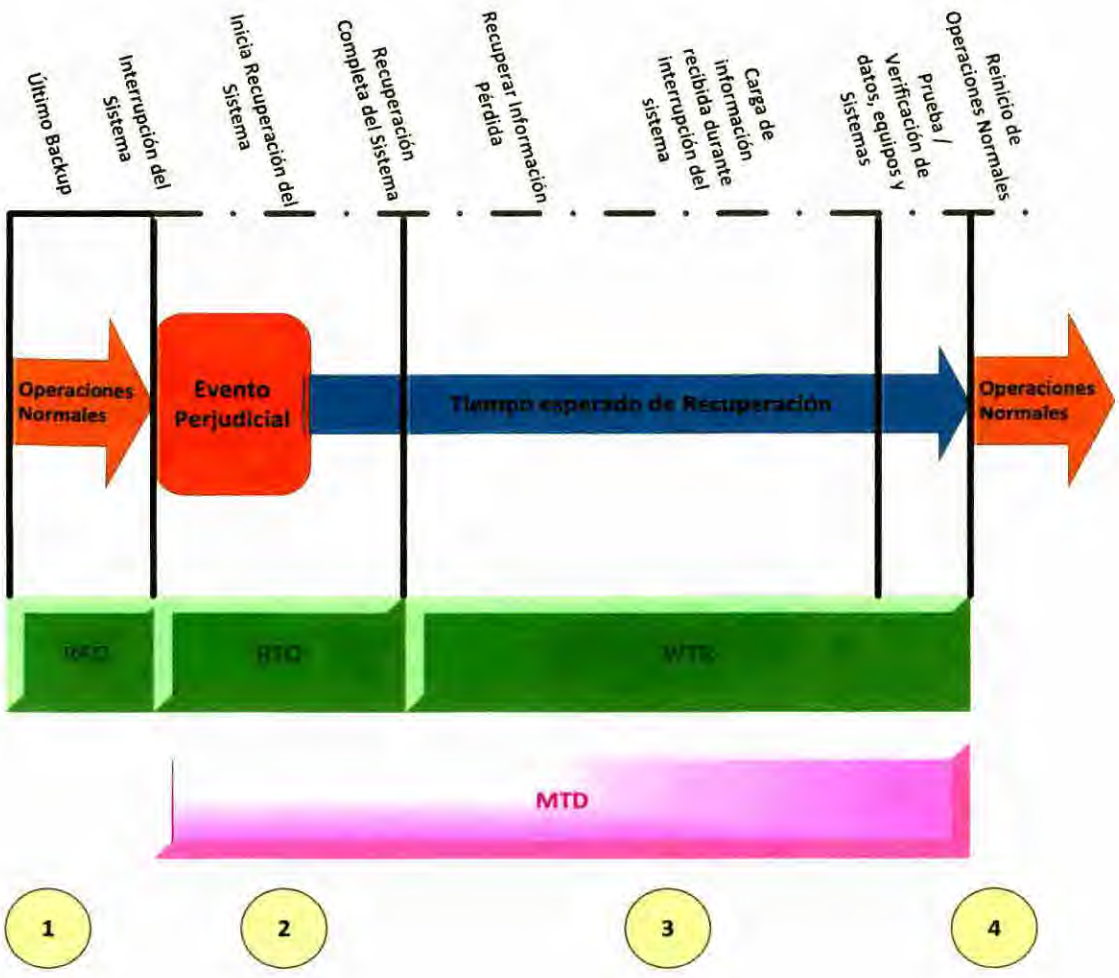
Si la institución llegase a realizar transacciones en linea (a traves de internet) el tiempo RPO tendria que ser cero ya que se necesitaria hasta el ultimo movimiento o transacción realizado por el cliente Razon por la cual el tiempo RPO nos indicaria la protección que debemos tener para el manejo y resguardo de la informacion Entonces el PRO y el RTO tienen influencia en el tipo de infraestructura necesaria para respaldar y dar soporte que se utilice la institucion

EL MTD Maximum Tolerable Downtime considerado como el máximo tiempo inactivo que una institucion u organización soporta la ausencia de uno de sus procesos criticos En una organizacion o institución pueden darse diversos MTD ya que esto depende del proceso o tarea al que se refiera Si un proceso en una institucion es categorizado con nivel de criticidad 1 el tiempo MTD tendria que ser muy pequeño Debemos tener en cuenta que cuando exista un nivel de criticidad mayor el tiempo para reiniciar la operación debe ser el menor posible

La conformación del tiempo inoperable está constituido por dos componentes el RTO (Recovery Time Objetive) y el WRT (Work Recovery Time) o Tiempo de Trabajo en Recuperación La fórmula para el cálculo del MTD seria de la siguiente manera (MTD = RTO + WRT) Si su MTD es de 24 horas probablemente 8 horas corresponden al RTO y las otras 16 horas pueden ser los WRT

En la Figura 5 observaremos cómo interactuan estos tiempos esta informacion ha sido obtenida del articulo Analisis de Impacto del Negocio publicado en el 30 de Mayo de 2010 por Leonardo Camelo

Figura 5. Tiempos RPO, RTO, WRT y MTD del BIA de los procesos.



Punto 1: El RPO es considerado como la cantidad máxima de datos que se permite malograr según el cronograma de backup con que se cuente en la institución.

Punto 2: El RTO no es más que es el tiempo donde los equipos y sistemas del IFARHU retornan a su operación normal.

Punto 3: El WRT es el tiempo que se requiere para recobrar la data o información que ha perdido.

Entonces el MTD sería lo que dure el RTO y el WRT.

Punto 4: se ejecutan los procesos de prueba, se verifican y se inician las operaciones normales.

El formulario para la encuesta que se utilizará en el IFARHU para obtener los diferentes tiempos que forman parte del BIA lo describimos a continuación:

Tabla 11. Formulario y resultados de las encuestas para obtener información de los tiempos del BIA para los sistemas de información.

Sistema de Información	RPO (Horas)	RTO (Horas)	WRT (Horas)	MTD (Horas)
Sistema de Crédito	8	7	5	12
Sistema de Correo electrónico	12	8	8	16
Sistema de emisión de Planillas y cheques	16	16	8	24
Sistema de becas	21	16	14	30
Sistema de digitalización de expedientes	28	18	16	34

Esta información se obtiene a través de encuestas a los Jefes de áreas que operan y administran estos sistemas. En la Tabla 11 se observa el resumen y compendio de la encuesta realizada. Teniendo identificado los sistemas de información críticos y sus tiempos de impacto al negocio, también identificamos el análisis de impacto para los equipos críticos siendo los mismos que encontramos para los sistemas. Este análisis de tiempos para los equipos lo realizamos encuestando a los encargados del área de Soporte Técnico y al Director de Tecnología e Información, basándonos en los resultados de la encuesta para los sistemas de información críticos del IFARHU descritos en la Tabla 11. Como observan en la Tabla 12 el MTD se reduce para los equipos dado a que estos debes estar operativos antes de realizar las pruebas de funcionamiento en el sitio alterno donde se alojen estos equipos.

Tabla 12. Formulario y sus resultados, utilizado para obtener información de los tiempos del BIA para los equipos que soportan los sistemas de información.

Los números del 1 al 6 indicados en la Tabla 12 se referencian a los equipos que soportan estos sistemas de la Tabla 10.

Equipos	RPO (Horas)	RTO (Horas)	WRT (Horas)	MTD (Horas)
1. Equipos para el Directorio Activo y	4	2	2	4

DHCP				
2. Equipos que soportan el Sistema de Crédito	8	4	4	8
3. Equipos Sistema de Correo electrónico	12	6	6	12
4. Equipos Sistema de emisión de Planillas y cheques	16	10	6	16
5. Equipos Sistema de becas	21	12	8	20
6. Equipos Sistema de digitalización de expedientes	28	14	10	24

3.2 IDENTIFICACIÓN DE POSIBLES RIESGOS / AMENAZAS NATURALES.

El P09 de Cobit (Evaluar y Administrar los Riesgos de TI) nos indica que para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados.

Los riesgos que amenazan el centro de cómputo del IFARHU y a la información que se procesa en esta institución fueron identificados por personal del departamento de Soporte Técnico del IFARHU en conjunto con la Dirección y Subdirección de TI y se pueden clasificar en dos grandes grupos:

3.2.1 EXTERNOS.

Son todos aquellos que se presentan en el ambiente que rodea a una instalación del centro de cómputo del IFARHU, por ejemplo (como ya se mencionó en la sección 2.1.6):

- Inundaciones.
- Movimientos Sísmicos (Temblores).
- Tornados
- Tormentas tropicales.
- Sabotaje.
- Motines Sociales.
- Robo (externo).
- Fallas de energía eléctrica.
- Huracanes
- Maremotos
- Ataques de Virus Informáticos

- Fuego en alrededores del centro de cómputo.
- Daño en los enlaces de comunicación.
- Cierre o paralización de las compañías proveedoras de servicios.
- Cierre o paralización de las compañías proveedoras de suministros de cómputo.

De los riesgos externos que pueden convertirse en las amenazas más comunes en Panamá y que puedan tener efectos que alteren los servicios que se ofrecen a través del centro de cómputo del IFARHU tenemos:

- ✓ Las Tormentas Tropicales.
- ✓ Inundaciones
- ✓ Fallas en la energía eléctrica.

3.2.2 INTERNOS.

Son los generados dentro de las instalaciones del IFARHU y en el centro de cómputo, por ejemplo:

- Daños en los equipos.
- Fuego interno (Centro de Cómputo o instalaciones que afecten el área o equipos tecnológicos).
- Equivocaciones de los usuarios del centro de cómputo, provocando daño a equipos, programas, archivos, datos, etc.
- Equivocaciones del personal del centro de cómputo, provocando daño a equipos, programas, archivos, etc.
- Alteraciones o fallas en la energía eléctrica interna.

Inundaciones internas

Falta de aire acondicionado

Daño en los UPS

Virus informáticos traidos en USB de sus casas o fuentes externas[24]

Acceso a informacion no autorizada

Robo de datos por funcionarios o personal de informatica

Robo interno comun llevándose equipos y/o archivos

Fallas en el cableado estructurado

Fallas en los Softwares de Aplicación (Microsoft Office Sistemas Operativos)

Fallas en los equipos

Falta de actualización de software de aplicación

Falta de actualización de equipos

De los riesgos internos que pudiesen convertirse en las amenazas más comunes en edificios como en el que se encuentra el centro de cómputo del IFARHU y que puedan tener efectos que alteren los servicios que se ofrecen tenemos

- ✓ Inundaciones internas
- ✓ Alteraciones o fallas en la energia electrica interna

[24] Pueden ser dispositivos que vienen de afuera de la institución (CD s discos duros externos correos electrónicos etc)

Ponderación del Riesgo

En esta se determina la vulnerabilidad de los sistemas o equipos estableciendo los adecuados niveles de calificación tanto del impacto como el de la probabilidad de ocurrencia Con lo anterior determinamos que tan vulnerable es el centro de cómputo del IFARHU ante situaciones previsibles Otros aspectos que se deben considerar son

- **La probabilidad con que ocurren los riesgos** determinaremos la probabilidad de ocurrencia considerando los controles que se utilizan actualmente y que tan efectivos sean al igual que con que frecuencia son materializados estos riesgos

- **Impacto** las consecuencias son evaluadas si el caso que da origen al riesgo es materializado

Los riesgos después de realizada su ponderación se deben manejar Existen varias posibilidades para su manejo las cuales describo a continuacion

- Evitarlo modificando los procesos o actividades que generan los riesgos
- Reducirlo aplicando controles para reducir la probabilidad o el impacto
- Transferirlo trasladarlo a otros departamentos de la institución o comprando pólizas para asegurarlo
- Compartir o diversificarlo es distribuirlo
- Asumirlo es aceptar el riesgo dado que el costo /beneficio de aplicar los controles son mayores a que se produzca el riesgo

3.2.3 MATRIZ DE RIESGO.

En la siguiente matriz, se describen los riesgos que pueden afectar los sistemas y equipos, provocando degradar los servicios que presta el centro de cómputo del IFARHU a los usuarios. La misma ha sido desarrollada en base a la identificación de riesgos descrita en el punto anterior. Para cada elemento que compone la matriz se determina la probabilidad del factor de riesgo. Además, a la matriz de riegos hemos incorporado la probabilidad de ocurrencia de los desastres naturales. Los que se identificaron en las instalaciones del centro de cómputo del IFARHU son los siguientes:

- Factor de riesgo **Bajo**. Probabilidad de ocurrencia de 0 a 1.
- Factor de riesgo **Medio**. Probabilidad de ocurrencia de 2 a 3.
- Factor de riesgo **Alto**. Probabilidad de ocurrencia mayor a 3.

Tabla 13. Identifica la Matriz de Riesgo Externo y la probabilidad de ocurrencia.

Descripción del Riesgo Externo	Factor de Riesgo	Probabilidad de Ocurrencia
Inundaciones.	Medio	3
Desertificación.	Bajo	0
Sequía	Bajo	1
Erosión y sedimentación	Bajo	0
Desbordamientos de ríos	Alto	4
Granizo	Bajo	0

Huracanes	**Bajo**	**1**
Tornados	**Medio**	**3**
Tormentas tropicales	**Alto**	**4**
Descargas eléctricas causadas por rayos	**Alto**	**4**
Fallas geológicas	**Bajo**	**1**
Terremotos	**Bajo**	**1**
Tsunamis	**Bajo**	**0**
Erupciones Volcánicas	**Bajo**	**0**
Incendios en Matorrales	**Medio**	**2**
Incendios en Sabanas	**Medio**	**2**
Motines Sociales	**Bajo**	**1**
Robo Externo	**Medio**	**2**
Ataques de Virus Informáticos	**Alto**	**4**
Fuego en los alrededores del centro de cómputo	**Medio**	**2**
Daños en los enlaces de comunicación	**Medio**	**2**
Cierre o paralización de las compañías proveedoras de servicios	**Medio**	**2**
Cierre o paralización de compañías proveedoras de materiales de cómputo	**Medio**	**3**

Tabla 14. Identifica la Matriz de Riesgo Interno y la probabilidad de ocurrencia.

Descripción del Riesgo Interno	Factor de Riesgo	Probabilidad de Ocurrencia
Inundaciones en edificios causadas por rupturas de tuberías, filtraciones por lluvia.	**Alto**	**5**
Daños en los equipos.	**Medio**	**3**
Fuego interno (Centro de Cómputo o instalaciones que afecten el área o equipos tecnológicos)	**Bajo**	**0**
Equivocaciones de los usuarios del centro de cómputo, provocando daño a equipos, programas, archivos, datos, etc.	**Medio**	**2**
Equivocaciones del personal del centro de cómputo, provocando daño a equipos, programas, archivos, etc.	**Bajo**	**1**
Alteraciones o fallas en la energía eléctrica interna.	**Alta**	**4**
Inundaciones internas	**Alta**	**4**
Falta de aire acondicionado.	**Medio**	**2**
Daños en los UPS	**Medio**	**3**
Virus informáticos traídos en USB de sus casas o	**Medio**	**2**

fuentes externas.		
Acceso a información no autorizada	**Bajo**	**0**
Robo de datos por funcionarios o personal de informática.	**Bajo**	**0**
Robo interno común, llevándose equipos y/o archivos	**Bajo**	**1**
Fallas en el cableado estructurado.	**Bajo**	**1**
Fallas en los Software de Aplicación. (Office XP, Sistemas Operativos).	**Bajo**	**1**
Falta de actualización de software de aplicación.	**Medio**	**2**
Falta de actualización de equipos de cómputo	**Medio**	**2**

En las tablas 13 y 14 el factor de riesgo es clasificado en bajo, medio y alto. Esta referencia es producto de consultas realizadas al personal del área de Soporte y Redes del Centro de cómputo del IFARHU, donde se les preguntó si la descripción de los riesgos internos y externos había ocurrido en los últimos 10 años. Definimos que para la existencia de un factor de riesgo bajo es cuando la descripción del riesgo nunca se ha materializado en este lapso de tiempo, es medio cuando su materialización en este tiempo es de una a tres veces, y es alto cuando su ocurrencia es de más de tres veces en este periodo.

De las dos matrices de riesgos presentadas en las Tablas 13 y 14 las dos amenazas naturales que pueden afectar la continuidad de los servicios ofrecidos en el centro de cómputo del IFARHU tenemos:

1. Tormentas tropicales.
2. Inundaciones internas.

Las tormentas tropicales afectan el centro de cómputo dado que producto de la gran cantidad de precipitación de agua y vientos que producen afectan el funcionamiento de los enlaces de comunicaciones y equipos de comunicación. En el centro de cómputo del IFARHU se encuentran ventanas que se pueden afectar e introducir agua, vientos y humedad que afecten los equipos y sistemas.

Otro aspecto que producen estas tormentas tropicales son las descargas eléctricas (rayos) que han afectado el suministro eléctrico y paralizado el funcionamiento del centro de cómputo por más de 10 horas, hasta que se halla restablecido el sistema eléctrico.

3.2.2 PROBABILIDADES DE OCURRENCIA DE LOS DESASTRES NATURALES.

Primeramente los desastres naturales son alteraciones intensas de las personas, los bienes, los servicios y el medio ambiente, causadas por un suceso natural, que exceden la capacidad de respuesta de la comunidad afectada. Son los desastres producidos por la fuerza de la naturaleza.

En la Tabla 13 se describe una lista de posibles desastres naturales y las probabilidades de que estos ocurran en nuestro pais y que pueden afectar el centro de cómputo del IFARHU Esta determinación fue realizada en consenso por los jefes de departamento de la Dirección de Tecnologia Informatica del IFARHU Para determinar la probabilidad de ocurrencia, se basaron en las veces que han ocurrido fenómenos similares a los descritos en nuestro pais en los ultimos 10 anos y que han afectado el servicio de cómputo del IFARHU o de otras instituciones gubernamentales en Panamá La misma tiene un rango de probabilidad de ocurrencia de 0 a 5 donde 0 es el rango más bajo y 5 el mas alto

Como se observa en la tabla 14 se describen las probabilidades de ocurrencia de los riesgos internos aunque muchos de estos no son causados por desastres naturales si pueden afectar el funcionamiento del centro de cómputo del IFARHU De lo anterior podemos observar que las inundaciones en edificios producidas por lluvias tormentas tropicales descargas eléctricas e incendios en edificios son las comunes en nuestro pais

3.3 PROTECCIÓN DE LOS CENTROS DE CÓMPUTO CONTRA AMENAZAS NATURALES.

Como el desarrollo del DRP de IFARHU está enmarcado hacia amenazas naturales, el centro de cómputo donde se alojan estos equipos debe contar con niveles de seguridad física que asegure la capacidad de supervivencia de la institución ante fenómenos naturales que pongan en peligro el centro de cómputo y por ende los servicios que los sistemas de información prestan a la institución. La seguridad física de esta área (Centro de cómputo del IFARHU) debe proteger y conservar los activos (equipos y programas) alojados en la misma, de riesgos, de desastres naturales o de actos involuntarios o mal intencionados. Debemos asegurar que existan controles adecuados para las condiciones ambientales que minimicen los riesgos por fallas o por mal funcionamiento del equipo, del software, de los datos y de los medios de almacenamiento.

El DRP del IFARHU debe contar con medidas de seguridad ambientales que ayuden a reducir los riesgos que se producen producto de estos fenómenos naturales, estas medidas las describo a continuación:

Incendios: estos son causados por el inadecuado uso de materiales combustibles en el centro de cómputo o en los alrededores del área, por fallas en las instalaciones eléctricas defectuosas. Para evitarlos se debe tener el área libre de material combustible e instalaciones eléctricas certificadas por personal idóneo.

Inundaciones: se refiere a la invasión de agua o derramamiento de la misma en el centro de cómputo. Lo anterior es producto de que se cuenta con lugares cercanos a los centros de cómputos con áreas para baños, inodoros, tuberías de aguas negras, tuberías de agua

potable que pasan cerca del centro de cómputo y que cualquier desperfecto en estas instalaciones produce derramamiento de agua También se originan inundaciones producto de tormentas tropicales y lluvias y en donde el area no cuenta con instalaciones adecuadas que producen estos derramamientos dentro del centro de computo Esta es una de las causas de mayores desastres en centros de cómputo Para evitar inundaciones debemos contar con instalaciones donde lo antes expuesto no forme parte de la misma, además dejarlo como politica de Departamento de Tecnologia para que se considere cuando se hagan revisiones fisicas de las áreas de la Institución

Humedad debemos contar con un medidor de temperatura y humedad que se encuentre en el centro de cómputo y que detecte cambios que afecten el funcionamiento de los equipos alojados en esta área y que nos envie alertas cuando uno de sus niveles normales sufran alteraciones

Temperatura el centro de cómputo del IFARHU cuenta con un sistema de aires acondicionados que dan soporte al area donde se encuentran los equipos Ademas cuenta con aires de contingencia en caso de que el aire principal sufra un desperfecto

Energía Eléctrica en nuestro pais dos son las fallas más comunes en el suministro de energia electrica

- Variaciones en el voltaje
- Interrupcion en el suministro eléctrico

Debido a que cualquiera de estos factores impacta en la continuidad de las operaciones el IFARHU cuenta con

- Utilizar UPS con reguladores de voltajes
- Equipo de suministro de energia alterno (Planta Electrica)

3.4 SITIO ALTERNO PARA RECUPERACIÓN DE DESASTRES.

Es fundamental para una institución como el IFARHU contar con un sitio alterno de trabajo. Generalmente los DRP requieren de sitios alternos donde se llevará a cabo la Recuperación. Un Sitio Alterno es una localidad o área de trabajo lo suficientemente distante del original como para no verse afectado por el mismo desastre que impacte el sitio principal.

Existen en Panamá dos tipos de Sitios Alternos según su uso, para equipo de cómputo y para funciones de oficina. El primero debe contar con todas las condiciones de clima, temperatura, energía eléctrica, sistemas de comunicación y de seguridad que tiene el original, el equipo de cómputo y la capacidad de las comunicaciones será en base a lo que determine el Análisis de Impacto en cuanto al mínimo de recursos funcional para las aplicaciones y equipos críticos. El segundo corresponde a las áreas de trabajo del personal operativo de la institución, el cual no está dentro del alcance de este DRP, ya que sólo está dirigido para los sistemas y equipos críticos de la institución.

El propósito de este sitio alterno es continuar el servicio a los usuarios y que los inconvenientes que se presenten producto de un desastre no ocasionen una paralización de las actividades por un largo periodo de tiempo.

En la actualidad el IFARHU no cuenta con un sitio alterno donde colocar sus equipos y sistemas razón por la cual estará incluido en este desarrollo del DRP.

CAPÍTULO IV. PLAN DE RECUPERACIÓN DE DESASTRES PARA EL IFARHU ANTE AMENAZAS NATURALES.

4.1 RECURSO HUMANO REQUERIDO.

El alcance de esta guía del DRP para el IFARHU está orientado a los equipos críticos (servidores y almacenamiento), los cuales soportan a los sistemas críticos de la institución. Lo anterior nos lleva a contar con recurso humano interno y externo para llevar a cabo el DRP. Se ha creado un Equipo de Recuperación de Desastres en cual tiene asignada funciones y responsabilidades al momento de ejecutar del DRP.

4.1.1 RECURSO HUMANO INTERNO PARA RECUPERACIÓN DE DESASTRES.

Esta sección identifica a los equipos de personas internas en el IFARHU involucradas en el esfuerzo de recuperación del evento de desastre y sus responsabilidades asociadas. Las pautas consideradas para la conformación de estos equipos han sido los siguientes:

- Todo equipo debe estar conformado por un líder y un alterno o sustituto.
- Ninguna persona debe estar participando en más de un equipo cuyas tareas, durante la recuperación de un desastre, sean concurrentes.

- Todas las personas identificadas en el Equipo de Recuperación de Desastres, deben conocer las responsabilidades que tienen que asumir. De esta manera se minimiza las posibilidades de inoperatividad de los equipos debido a la ausencia de sus integrantes y/o al desconocimiento de sus responsabilidades.

Se ha conformado el siguiente Equipo de Recuperación de Desastres TI para el alcance identificado en la presente guía para el Plan de Recuperación de Desastres:

Figura 6. Organigrama del Equipo de Recuperación de Desastres interno del IFARHU

4.1.1.1 COORDINADOR DE RECUPERACIÓN DE TI (CRTI)

Tiene asignado las siguientes responsabilidades:

1. Encargado de coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
2. Tomar la decisión de activar el Plan de Recuperación de Desastres.
3. Proveer liderazgo general a los equipos de personas involucrados en el proceso de recuperación.
4. Guiar al personal necesario durante la situación de contingencia y supervisar sus actividades.
5. Evaluar la extensión del desastre y sus consecuencias potenciales sobre la infraestructura tecnológica.
6. Notificar, y mantener enterados, a la Alta Dirección acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
7. Documentar los eventos de desastres y las actividades realizadas para lograr la recuperación de las operaciones.
8. Monitorear la ejecución de los procedimientos de recuperación y asegurar que el cronograma y las prioridades establecidas se cumplan.
9. Supervisar / vigilar la recuperación de infraestructura de TI en el Centro de Datos alterno.

10. Contactar a los proveedores para el hardware de remplazo para sistemas afectados.

11. Asistir a las reuniones del estado de la recuperación y comunicar al personal las necesidades y prioridades.

12. Declarar el evento de término de la ejecución de las operaciones del Plan de Recuperación de Desastres, cuando las operaciones de los sitios de procesamiento primarios hayan sido restablecidas.

Ver ejemplo de las posiciones o cargos y personas asignadas a este rol en ANEXO A - Directorio del Equipo de Recuperación de Desastres.

4.1.1.2 COORDINADOR DE INFRAESTRUCTURA TECNOLÓGICA (CIT)

Tiene asignado las siguientes responsabilidades:

1. Evaluar el daño en la plataforma tecnológica básica del IFARHU, coordinar y dirigir las acciones necesarias para su recuperación en el Centro de Datos alterno y su restauración a condiciones normales.

2. Recuperar la plataforma base de acuerdo a la prioridad de recuperación definida en la Tabla 10, donde se describen los equipos críticos y su orden de criticidad.

3. Asegurar que toda la documentación relacionada a estándares, operaciones, registros vitales, programas de aplicación, procedimientos de instalación de

sistemas operativos utilitarios procedimientos de respaldo y recuperación etc se encuentren almacenados en un ambiente seguro

4 Mantener los procedimientos de operaciones actualizados

5 Mantener actualizado y en un lugar seguro (sitio alterno de recuperación) copia de la configuración de los equipos y sistemas

6 Supervisar la instalación del hardware y software base asi como configurar las ultimas versiones de los sistemas operativos en los ambientes del Centro de Datos alterno (esta ultima parte se está desarrollando en un DRP de las aplicaciones y sistemas)

7 Recuperar las cintas de respaldo del almacenaje externo y entregarlas al sitio de recuperación

8 Habilitar los procedimientos de backup y restablecer los controles normales de operación en los sitios primarios luego de restablecidos los servicios en dicho ambiente

9 Mantener recuperar y/o restaurar los enlaces de red y comunicaciones entre las sedes primarias del IFARHU y el Centro de Datos alterno (Partimos del supuesto que ya existen enlaces de comunicación entre el sitio principal y el sitio alterno ademas de los equipos de comunicacion Routers Switches y Firewall) el cableado interno en el centro de datos alterno y el cableado de red necesario

10. Mantener actualizado el diagrama actual de conexiones de dispositivos, el diagrama alterno y el inventario de equipos de telecomunicaciones a ser usado en caso de emergencia.
11. Evaluar el daño en las redes de comunicación de datos y coordinar las estrategias de recuperación con los proveedores de servicios.
12. Informar a los usuarios hasta qué momento se tienen datos confiables.
13. Asegurar que la documentación de los aplicativos en producción se mantenga actualizada y que la documentación de operaciones contemple las actividades de respaldo de los aplicativos.
14. Definir las actividades de recuperación para los casos de pérdida de información y/o contingencia.

Ver ejemplo de cargos y personas asignadas a este rol en ANEXO A - Directorio del Equipo de Recuperación de Desastres.

4.1.1.3 ASESOR EN SEGURIDAD INFORMÁTICA.

Tiene asignado las siguientes responsabilidades:

1. Supervisar el cumplimiento de los controles que permitan asegurar la integridad, confidencialidad y disponibilidad de la información durante la situación de contingencia.
2. Coordinar con los encargados de Seguridad Física de la institución, la evaluación del daño en los sitios primarios.

3. Coordinar la evaluación del DRP una vez activado y ejecutado, con miras a identificar las debilidades y fortalezas del plan.
4. Documentar la ejecución del DRP, para que la misma sea utilizada en la evaluación del plan.
5. Participar en el comité de mantenimiento del DRP, con miras a ayudar en las mejoras del Plan.

Ver ejemplos de cargos o posiciones asignadas a este rol en ANEXO A - Directorio del Equipo de Recuperación de Desastres.

4.1.2 RECURSO HUMANO EXTERNO.

El recurso humano externo es el personal de mantenimiento de los proveedores de servicio externo, el personal gerencial y mandos medios de estas empresas, los cuales cuando ocurra una contingencia con los equipos críticos, nos brindarán el soporte técnico. Este recurso humano externo nos apoyará presencialmente en el centro de datos alterno. Encontraremos un ejemplo del recurso humano externo descrito en el ANEXO E.

Otro aspecto importante en un DRP es llevar un eficiente control de los contratos de mantenimientos de los equipos críticos del centro de cómputo del IFARHU, lo cual nos permitirá contar con su soporte cuando tengamos eventualidades con estos equipos o cuando se active el DRP para el centro de cómputo.

Para llevar un control de los contratos activos del centro de cómputo del IFARHU se debe desarrollar una hoja de cálculo (en Excel) para identificar los nombres de los proveedores las fechas de vencimientos de los contratos la forma de renovacion los niveles de servicio y el sistema o equipo que ampara dicho contrato formulario este que no forma parte de este DRP pero que debe ser llevado por la Dirección de Tecnologia e Informática para apoyarse en su gestión de administración

4.2 ESTRATEGIA POSIBLE DE RECUPERACIÓN.

Debido a los tiempos de recuperación (RTO) para los equipos críticos, descritos anteriormente en la Tabla 12, es necesario contar con un Centro de Datos alterno que garantice la recuperación de los procesos críticos de la institución en el menor tiempo posible. Además en este centro de datos deben existir áreas de trabajo externas al centro de cómputo alterno, para que uno o dos de los colaboradores que operan cada sistema crítico puedan trabajar desde ese lugar, esto último no forma parte de este documento ya que se tendría que ver en un Plan de Continuidad de Negocios.

4.2.1 ESTRATEGIA PARA LA INFRAESTRUCTURA TECNOLÓGICA DE CONTINGENCIA.

Como parte plan de recuperación de desastres es necesario definir una estrategia para desplegar la infraestructura tecnológica que entrará en operación ante un escenario de contingencia. En tal sentido, analizando los RTOs anteriormente obtenidos se plantean la siguiente estrategia:

Estrategia:

Se considera un escenario total de desastre en el cual los servidores instalados en el sitio de procesamiento primario se tornan inoperables, por cuanto la alternativa de procesamiento debiera realizarse en el Centro Alterno.

4.2.2 RECURSOS NECESARIOS PARA IMPLEMENTAR LA ESTRATEGIA DE RECUPERACIÓN.

De acuerdo a las evaluaciones realizadas para el desarrollo de esta guía para el DRP de los equipos críticos del IFARHU, se debe contar con una infraestructura de contingencia en el sitio alterno semejante a la descrita en la Tabla 10 de esta guía. Lo anterior obedece a que sería lo óptimo para que exista un eficiente DRP.

De igual manera, el centro de datos alterno necesita contar con los siguientes equipos de comunicación y respaldo indicados en la **Tabla 15**.

Tabla 15. Equipos de Comunicación instalados y configurados en el sitio alterno del DRP.

Switch Alterno Pasivo, con la configuración y políticas idénticas a las del sitio primario
Firewall Alterno Pasivo, con la configuración y políticas idénticas a las del sitio primario
Router Alterno Pasivo, con la configuración y políticas idénticas a las del sitio primario
Solución de backup para restaurar las configuraciones sistemas, bases de datos y programas utilizados en el sitio primario del IFARHU.

Es importante que el centro alterno cuente con controles ambientales, como los siguientes, que se muestran en la **Tabla 16.**

Tabla 16. Controles ambientales con los que debe contar el sitio alterno.

Detectores de humo
Sensores de Temperatura
Extintores
Interruptor de corte de energía
Aire acondicionado
Piso falso / techo
Cableado debidamente etiquetado bajo el falso piso
Rack para servidores (con llave)
UPS

4.2.3 PROCEDIMIENTO DE ACTIVACIÓN DEL PLAN.

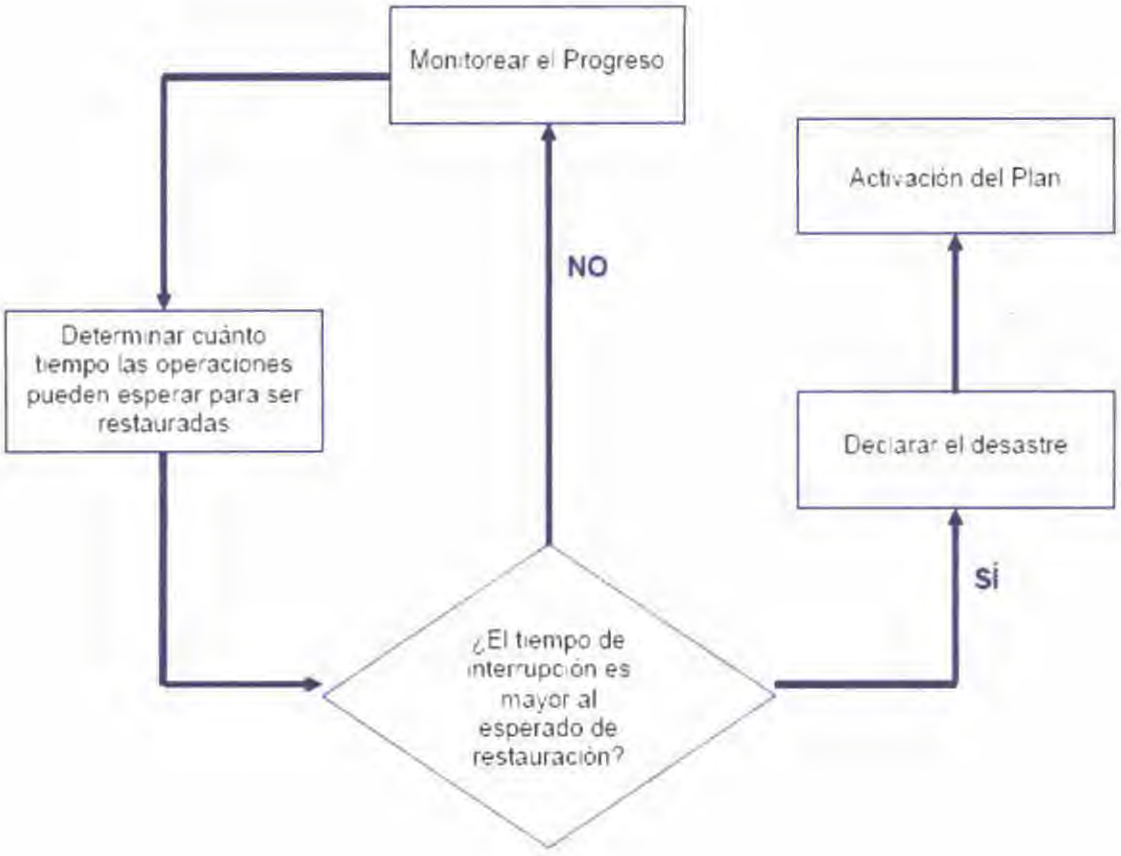
Este procedimiento tiene como objetivo evaluar el desastre al cual se ve enfrentada la infraestructura de servidores y almacenamiento ubicada en el centro de cómputo del IFARHU al no estar operable en el sitio primario, tomando las acciones correspondientes en caso de una situación de emergencia.

Equipo de Evaluación del Desastre, se ha conformado un equipo la evaluación de los posibles desastres el cual está integrado por:

- Coordinador de Recuperación de TI.
- Coordinador de Infraestructura Tecnológica.
- Asesor en seguridad.

El siguiente diagrama muestra los criterios que deberán ser usados para activar el Plan de Recuperación de Desastres.

Figura 7. Criterios que su utilizarán para activar el DRP de los equipos críticos del IFARHU



Se observa que una interrupción no es solamente un evento que reduce la efectividad de los sistemas, es un evento extraordinario que causa una pérdida de procesos de negocios clave y tiene un impacto alto en la institución.

4.2.3.1 SITUACIÓN DE EMERGENCIA.

Ante una situación de emergencia, se deberá proceder de la manera siguiente indicada en la Tabla 17.

Tabla 17. Procedimiento ante una situación de emergencia.

#	Acción	Descripción	Responsabilidad	Referencia	Check
1	Recibir Notificación	Cuando se presente una situación de emergencia, ésta deberá ser notificada al Coordinador de Recuperación de TI. Si la persona que detecta la emergencia no puede contactarse con el responsable, entonces deberá notificar uno a uno a los miembros del Equipo de Recuperación hasta poder contactarse con alguno de ellos.	Empleado de la Institución (IFARHU)	ANEXO A - Directorio del Equipo de Recuperación de Desastres	
2	Confirmar Notificación	Cuando la notificación de una contingencia potencial es recibida, se debe obtener	Coordinador de Recuperación de	N/A	

#	Acción	Descripción	Responsabilidad	Referencia	Check
		una descripción breve de la naturaleza del incidente y cualquier tipo de daño. Si es necesario, se debe confirmar que la notificación es verídica a través de un medio secundario. El medio secundario puede ser otra persona que presenció el hecho.	TI		
3	Contactar Servicios de Emergencia	Si la situación lo amerita, se deberá efectuar el contacto con los servicios de emergencia. Situaciones que pueden ser consideradas de emergencia son mencionadas anteriormente.	Coordinador de Recuperación de TI	ANEXO B – Directorio de Servicios de Emergencia	
4	Notificar a la seguridad del	Notificar inmediatamente al personal de seguridad del	Coordinador de Recuperación de	N/A	

#	Acción	Descripción	Responsabilidad	Referencia	Check
	IFARHU	IFARHU	TI		
5	Reunión de coordinación	Coordinar una reunión a la brevedad posible con el Equipo de Recuperación (descrito en la Figura 6), con la finalidad de hacer una evaluación preliminar de los daños.	Coordinador de Recuperación de TI	N/A	
6	Evaluar el Incidente	Evaluar el incidente de desastre y determinar la cantidad de tiempo requerido para completar la reparación. El daño ocasionado a la infraestructura y a las instalaciones deberá ser evaluado y documentado en el ANEXO C. (documento de salida)	Equipo de Evaluación del Desastre (Definido en el punto 4.2.3 de esta guía)	ANEXO C – Formato de Evaluación del Desastre	

#	Acción	Descripción	Responsabilidad	Referencia	Check
7	Declarar la Contingencia	En caso que el tiempo requerido para completar la reparación de los daños sea mayor al tiempo de recuperación requerido por el negocio, se declara la situación de emergencia y se da por activado el Plan de Recuperación de Desastres. Documentarlo en el ANEXO C. (documento de salida)	Equipo de Evaluación del Desastre	ANEXO C – Formato de Evaluación del Desastre	
8	Alistar los recursos requeridos para el Centro de Datos alterno	Proveer transporte para el equipo de recuperación, personas y suministros requeridos para el restablecimiento de las operaciones en el Centro de Datos alterno.	Coordinador de Recuperación de TI	N/A	
9	Alertar personal	Se debe alertar a todo los miembros del Equipo de Recuperación que no se	Coordinador de Recuperación de	ANEXO A - Directorio del Equipo de	

#	Acción	Descripción	Responsabilidad	Referencia	Check
	involucrado	encuentren presentes al momento de la declaración de la situación de emergencia. Progresivamente avisar y orientar al resto del personal de la empresa.	TI	Recuperación de Desastres	
10	Ejecutar el Procedimiento General de Recuperación	Iniciar las actividades de recuperación en el Centro de Datos alterno de acuerdo a los procedimientos de recuperación definidos más adelante. Este incidente debe ser registrado.	Coordinador de Recuperación de TI	N/A	

4.3 PROCEDIMIENTO GENERAL DE RECUPERACIÓN.

Este procedimiento general tiene como objetivo la activación del Centro de Datos alterno para el restablecimiento de la totalidad de los equipos tecnológicos requeridos para garantizar la continuidad de los procesos críticos del IFARHU, identificados como resultado del BIA. Es importante mencionar que existen procedimientos internos descritos con los que cuenta la Dirección de Tecnología Informática del IFARHU para instalación y recuperación de equipos (servidores, routers, switches, computadoras personales, etc,) que no están descritos en este documento pero que son apoyo para la implementación del DRP. Es responsabilidad de la Dirección de Tecnología Informática mantenerlos actualizados y disponibles para su utilización tanto en el sitio principal como en el alterno. A continuación se detallan las acciones que conforman el procedimiento general de recuperación indicado en la **Tabla 18.**

Tabla 18. Procedimiento General de Recuperación.

#	Acción	Descripción	Responsabilidad	Referencia	Evaluación EC/EP/NE	Documentar
1	Contactar al Equipo de Recuperació	El Equipo de Recuperación debe ser notificado y movilizado a las instalaciones	Coordinador de Recuperación	ANEXO A - Directorio del Equipo de		

#	Acción	Descripción	Responsabilidad	Referencia	Evaluación EC/EP/NE	Documentar
	n de TI	del Centro de Datos alterno.	TI	Recuperación de Desastres		
2	Notificar a la empresa encargada de la custodia de las cintas de respaldo para el restablecimiento de las mismas	Notificar a la empresa encargada de la custodia de las cintas de respaldo acerca de la situación de desastre, con el objetivo de que estén preparados para enviar las cintas de respaldo sin retrasos, según los acuerdos contractuales definidos, y en el lugar y tiempo acordado. Dejar constancia de la notificación. (documento de salida)	Coordinador de Infraestructura Tecnológica	ANEXO E – Directorio de Proveedores Externos		
3	Notificar al proveedor de comunicaciones	Notificar al proveedor de comunicaciones acerca de la situación de desastre e indicar que debe realizar cambios en la configuración, para trabajar desde el sitio alterno. Detallar la	Coordinador de Infraestructura Tecnológica	ANEXO E – Directorio de Proveedores Externos		

#	Acción	Descripción	Responsabilidad	Referencia	Evaluación EC/EP/NE	Documentar
		información que se ha perdido y debe ser recuperada. Dejar constancia de la notificación. (documento de salida)				
4	Activar el Centro de Datos alterno	Declarar el Centro de Datos alterno como Centro de Datos de contingencia. Se debe revisar el checklist del ANEXO D - Requisitos en el Centro de Datos Alterno. Adicionalmente, se deberá tener en cuenta los insumos, adicionales al HW y SW críticos, para el correcto funcionamiento del mismo.	Coordinador de Recuperación de TI	ANEXO D - Requisitos en el Centro de Datos Alterno		
5	Identificar la pérdida de plataforma tecnológica	Utilizar la Tabla 10 - Inventario de equipos Críticos para identificar la infraestructura tecnológica perdida en el Centro de Datos primario y generar	Coordinador de Infraestructura Tecnológica y Coordinador	Tabla 10 Inventario de equipos Críticos y		

#	Acción	Descripción	Responsabilidad	Referencia	Evaluación EC/EP/NE	Documentar
		informe. (documento de salida)	de sistemas de Información	Anexo C		
6	Determinar los equipos que pueden ser reutilizados	Determinar equipos que puedan ser reutilizados luego de la contingencia. Revisar su operatividad, y confiabilidad, para validar que la misma no se haya visto afectada como consecuencia del evento de desastre ocurrido en el Centro de Datos primario. Generar informe con los equipos a reutilizar. (documento de salida)	Coordinador de Infraestructura Tecnológica y Coordinador de sistemas de Información	Tabla 10 Inventario de equipos Críticos y Anexo C		
7	Determinar necesidades adicionales y coordinar adquisiciones de	Determinar los elementos adicionales que son necesarios para facilitar la recuperación de los procesos críticos. Estos artículos se deben comprar inmediatamente. Generar informe con los elementos	Coordinador de Infraestructura Tecnológica y Coordinador de sistemas de	N/A		

#	Acción	Descripción	Responsabilidad	Referencia	Evaluación EC/EP/NE	Documentar
	emergencia.	adicionales adjuntando el ANEXO F – Reporte Equipos Evaluados como sustento de las compras solicitadas. (Documento de salida). Es importante definir los requerimientos necesarios para dejar el centro de datos de contingencia operativos. Considerar así mismo los contratos de seguros actuales.	Información			
8	Recuperar copias de seguridad de aplicaciones	(Documento de entrada: informes de los puntos 5 y 6). Recuperar, de ser necesarias las copias de seguridad, ya sean del Centro de Datos o en su defecto del almacenamiento externo y restaurar la información (documento de salida).	Coordinador de Infraestructura Tecnológica	N/A		

#	Acción	Descripción	Responsabilidad	Referencia	Evaluación EC/EP/NI	Documentar
9	Preparar la plataforma tecnológica para la recuperación de los procesos	(Documento de entrada: informes de los puntos 5 y 6). De ser necesario coordinar, la instalación de software base, aplicar parches, restaurar los últimos backups de configuración y aplicar scripts de recuperación, sobre la plataforma tecnológica del Centro de Datos alterno (documento de salida). Para ejecutar estos procesos nos apoyaremos en los procedimientos internos desarrollados por la Dirección de Tecnología y los provistos por los proveedores de estos equipos.	Coordinador de Infraestructura Tecnológica Coordinador de Sistemas de Información	Manual de Procedimientos de la Dirección de Tecnología del IFARHU. Instructivo de instalación de los equipos provistos por los proveedores.		
1	Recuperar el Dominio de	Ejecutar el procedimiento de recuperación del Dominio de	Coordinador de	PROCEDIMIENTO –		

#	Acción	Descripción	Responsabilidad	Referencia	Evaluación EC/EP/NE	Documentar
0	Red	Red	Infraestructura tecnológica	Dominio de Red		

EC = Ejecución Completa de la acción

EP = Ejecución Parcial de la acción.

NE = No se ejecutó la acción.

Aclaramos que el paso 10 del procedimiento de Recuperación General de Recuperación descrito en la Tabla 19, sólo se ejecutará de manera exclusiva para el Servidor de Dominio.

Este procedimiento General de Recuperación puede ser utilizado para recuperar los otros servidores críticos en el centro alterno, sólo que debemos considerar la no ejecución del paso 10 para estos otros servidores.

El orden de recuperación de estos servidores en el sitio alterno es el que describimos a continuación:

1. Servidor de Red.
2. Servidor del Sistema de Crédito.
3. Servidor de Correo electrónico.

4 Servidor del Sistema de Planillas y Cheques y su unidad de almacenamiento (SAN) Para instalar el SAN en el sitio alterno se depende de los conocimientos del proveedor (DELL) para lo cual debemos utilizar el Anexo E (Proveedores Externos) para localizarlo y que procedan con la instalación y restauración de este equipo Por lo cual existe dependencia del proveedor

5 Servidor de Becas

6 Servidor del Sistema de Imagenes

Cuando se encuentren instalados y configurados los equipos criticos en el sitio alterno se debe proceder con la otra parte del Plan de Recuperacion de Desastres de las Aplicaciones y Bases de Datos la cual se encuentra desarrollada en otro documento o guia para este fin

4.4 PROCEDIMIENTOS DE RECUPERACIÓN DE DOMINIO DE RED.

Ante un desastre en el Centro de Datos principal sería necesario restaurar un servidor con los servicios de dominio en el Centro de Datos alterno para dar servicio a los usuarios del IFARHU. Partimos del hecho de que ya existe un servidor en el sitio alterno con características iguales al del sitio principal.

Equipo Participante:

- Coordinador de Infraestructura tecnológica:
    - Equipo de Controlador de Dominio
    - Equipo de Comunicaciones

Tabla 19. Procedimiento de recuperación del Dominio de la RED.

#	Acción	Descripción	Responsabilidad	Evaluación EC/EP/NE	Documentar
1	Recuperar Cintas	Recuperar las cintas de backup desde el sitio de almacenamiento	Operador Backup / Restore		
2	Verificar cintas	Verificar las fechas de las cintas que se correspondan con la fecha del resguardo más reciente.	Operador Backup / Restore		
3	Instalar el Sistema Operativo	Instalar la versión Windows Server 2003 R2 desde los CDs de instalación del producto.	Soporte Técnico, Servidores y HW, Operador Backup		

	Windows Server		/ Restore		
4	Realizar la restauración	Por medio de la herramienta NT Backup de Windows Server restaurar el backup de la cinta, del último system state más cercano a ese día.	Operador Backup / Restore		
5	Arrancar el Sistema Operativo en modo SD (Servicio de directorio)	Arrancar el sistema operativo en modo de recuperación del controlador de dominio presionando F8 y seleccionando la opción arrancar en modo restauración de SD.	Servidores y HW, Soporte Técnico		
6	Ejecutar proceso de restauración	Ejecutar la restauración, indicando la ubicación del backup del system restore (paso 4) *Ver Instructivo a continuación *	Operador Backup / Restore		
7	Iniciar el servidor	Iniciar el controlador de dominio	Servidores y HW, Soporte Técnico		
8	Verificar las configuraciones	Verificar los servicios en ejecución y las configuraciones del sistema	Servidores y HW, Soporte Técnico		
9	Verificar conexión	Verificar la conectividad del servidor local y remota.	Comunicaciones y Servidores y HW		
10	Informar sobre la ejecución del proceso	Generar informe adjuntando el presente procedimiento con el objetivo de dejar constancia de las acciones realizadas.	Servidores y HW, Soporte Técnico		

4.4.1 INSTRUCTIVO – RESTAURAR DATOS DE ESTADO DEL SISTEMA

Para restaurar datos de Estado del sistema

1. Abra Copia de seguridad.

El Asistente para copia de seguridad o restauración se inicia de forma predeterminada, salvo que esté deshabilitado

2 Haga clic en el vínculo Modo avanzado del Asistente para copia de seguridad o restauracion

3 Haga clic en la ficha Restaurar y administrar medios y haga clic en la casilla situada junto a Estado del sistema De esta forma, se realizará la restauración de los datos de Estado del sistema junto con cualquier otro dato que haya seleccionado para la presente operación de restauración

Notas

- Para llevar a cabo este procedimiento debe ser miembro del grupo Administradores en el equipo local o tener delegada la autoridad correspondiente Si el equipo está unido a un dominio los miembros del grupo Administradores de dominio podrían llevar a cabo este procedimiento Como práctica recomendada de seguridad considere la posibilidad de utilizar la opción Ejecutar como para llevar a cabo este procedimiento
- Para iniciar Copia de seguridad haga clic en Inicio seleccione Todos los programas Accesorios Herramientas del sistema y a continuacion haga clic en Copia de seguridad

- También puede restaurar los datos de Estado del sistema mediante el Asistente para restauracion para ello haga clic en Asistente para restauracion en el menu Herramientas
- Si va a restaurar los datos de Estado del sistema en un controlador de dominio debe elegir si desea realizar una restauracion primaria una restauración autoritaria o una restauración no autoritaria El método predeterminado de restauración de los datos del Estado del sistema en un controlador de dominio es el modo no autoritario (normal) En este modo cualquier componente de Estado del sistema que se encuentre replicado en otro controlador de dominio como el servicio de directorio de Active Directory o el servicio de Replicación de archivos (incluido el directorio SYSVOL) se actualizará mediante replicacion una vez restaurados los datos Por ejemplo si la ultima copia de seguridad se realizó hace una semana y se ha restaurado el Estado del sistema utilizando el metodo de restauración predeterminado (no autoritario) cualquier cambio realizado posteriormente a la operación de copia de seguridad se replicara desde los controladores de dominio
- En algunos casos puede no ser aconsejable replicar los cambios que se hayan podido realizar con posterioridad a la ultima operación de copia de seguridad En otras palabras puede haber ocasiones en las que desee que todas las réplicas tengan el mismo estado que los datos de la copia de seguridad Para alcanzar este estado debe ejecutar una restauración autoritaria
- Por ejemplo tendrá que ejecutar una restauración autoritaria si de forma inadvertida, elimina usuarios grupos o unidades organizativas del servicio de directorio de Active Directory y desea restaurar el sistema para recuperar y

replicar los objetos eliminados Para ello tendrá que ejecutar la utilidad Ntdsutil después de restaurar los datos pero antes de reiniciar el controlador de dominio Esta utilidad permite marcar objetos como autorizados lo que asegura que cualquier dato replicado o distribuido que haya restaurado se replicara o distribuirá adecuadamente en toda la organización La utilidad de linea de comandos Ntdsutil se puede ejecutar desde el simbolo del sistema Para obtener Ayuda acerca de la utilidad Ntdsutil en el simbolo del sistema, escriba ntdsutil /? Para obtener más informacion vea Temas relacionados

- Para restaurar los datos de Estado del sistema en un controlador de dominio debera iniciar antes el equipo con una opcion de inicio especial denominada Modo de restauración de servicios de directorio Esto le permitirá restaurar el directorio SYSVOL y la base de datos del servicio de directorio Active Directory Para tener acceso al Modo de restauración de servicios de directorio presione F8 durante el inicio y seleccionelo en la lista de opciones de inicio Para obtener más información acerca de las opciones de inicio vea Temas relacionados

Sólo puede restaurar los datos de Estado del sistema en un equipo local No puede restaurar los datos de Estado del sistema en un equipo remoto

4.5 RESTABLECIMIENTO DE LAS CONDICIONES NORMALES.

Este procedimiento general tiene como objetivo el restablecer las condiciones normales de operación en el Centro de Datos principal una vez que se puede dejar el escenario de contingencia. Es importante mencionar que este procedimiento es similar al procedimiento general de recuperación pero con la diferencia que los procedimientos son realizados sobre el centro de datos principal.

A continuación en la **Tabla 20**, se detallan las acciones que conforman del restablecimiento de las condiciones normales.

Tabla 19. Procedimiento para restablecer a las condiciones normales.

#	Acción	Descripción	Responsa-bilidad	Referencia	Evaluación EC/EP/NE	Documentar
1	Contactar al Equipo de Recuperación de TI	El Equipo de Recuperación será en encargado de retornar a las condiciones normales de operación para lo cual debe ser notificado y movilizado a las instalaciones del Centro de Datos principal.	Coordinador de Recuperación TI	ANEXO A - Directorio del Equipo de Recuperación de Desastres		
2	Notificar a la empresa	Notificar a la empresa encargada de la custodia	Coordinador de	ANEXO E – Directorio		

#	Acción	Descripción	Responsa-bilidad	Referencia	Evaluación EC/EP/NE	Documentar
	encargada de la custodia de las cintas de respaldo para el restablecimiento de las mismas en el Centro de Cómputo Principal del IFARHU	de las cintas de respaldo nuevamente, con el objetivo de que estén preparados para enviar las cintas de respaldo sin retrasos, según los acuerdos contractuales definidos, y en el lugar y tiempo acordado. Dejar constancia de la notificación. (documento de salida)	Infraestructura Tecnológica	de Proveedores Externos		
3	Notificar al proveedor de comunicaciones	Notificar al proveedor de comunicaciones indicando que se debe volver a las condiciones normales en el sitio principal y que para que realice los cambios en la configuración. Dejar constancia de la notificación. (documento	Coordinador de Infraestructura Tecnológica	ANEXO E – Directorio de Proveedores		

#	Acción	Descripción	Responsa-bilidad	Referencia	Evaluación EC/EP/NE	Documentar
		de salida)				
4	Activar el Centro de Datos primario	Activar el Centro de Datos primario.	Coordinador de Recuperación de TI			
5	Identificar la pérdida de plataforma tecnológica	Utilizar la Tabla 10 - Inventario de Equipos Críticos, para identificar la infraestructura tecnológica que se recuperará en el Centro de Datos primario y generar informe. (documento de salida)	Coordinador de Infraestructura Tecnológica y Coordinador de sistemas de Información	Tabla 10 Inventario de equipos Críticos y Anexo C		
6	Determinar los equipos que pueden ser reutilizados	Determinar equipos que puedan ser reutilizados luego de la contingencia. Revisar su operatividad, y confiabilidad, para validar	Coordinador de Infraestructura Tecnológic	Tabla 10 Inventario de equipos Críticos y Anexo C		

#	Acción	Descripción	Responsa-bilidad	Referencia	Evaluación EC/EP/NE	Documentar
		que la misma no se haya visto afectada como consecuencia del evento de desastre ocurrido en el Centro de Datos primario. Generar informe con los equipos a reutilizar. (documento de salida)	a y Coordinador de sistemas de Información			
7	Determinar necesidades adicionales y coordinar adquisiciones de emergencia	Determinar los elementos adicionales que son necesarios para facilitar la recuperación de los procesos criticos. Estos artículos se deben comprar inmediatamente. Generar informe con los elementos adicionales adjuntando el ANEXO F – Reporte Equipos Evaluados como sustento de las compras solicitadas. (Documento de salida). Es importante	Coordinador de Infraestructura Tecnológica y Coordinador de sistemas de Información	N/A		

#	Acción	Descripción	Responsa-bilidad	Referencia	Evaluación EC/EP/NE	Documentar
		definir los requerimientos necesarios para dejar el centro de datos primario operativo. Considerar así mismo los contratos de seguros actuales.				
8	Recuperar copias de seguridad de aplicaciones	(Documento de entrada: informes de los puntos 5 y 6). Recuperar, de ser necesarias las copias de seguridad, ya sean del Centro de Datos o en su defecto del almacenamiento externo y restaurar la información (documento de salida).	Coordinador de Infraestructura Tecnológica	N/A		
9	Preparar la plataforma tecnológica para la	(Documento de entrada: informes de los puntos 5 y 6). De ser necesario coordinar,	Coordinador de Infraestructura	Manual de Procedimientos de la Dirección de		

#	Acción	Descripción	Responsa-bilidad	Referencia	Evaluación EC/EP/NE	Documentar
	recuperación de los procesos	la instalación de software base, aplicar parches, restaurar los últimos backups de configuración y aplicar scripts de recuperación, sobre la plataforma tecnológica del Centro de Datos primario (documento de salida). Para ejecutar estos procesos nos apoyaremos en los procedimientos internos desarrollados por la Dirección de Tecnología y los provistos por los proveedores de estos equipos.	Tecnológica Coordinador de Sistemas de Información	Tecnología del IFARHU. Instructivo de instalación de los equipos provistos por los proveedores.		
10	Recuperar el Dominio de Red	Ejecutar el procedimiento de recuperación del Dominio de Red. Este procedimiento debe ser	Coordinador de Infraestructura	PROCEDIMIENTO – Dominio de Red		

#	Acción	Descripción	Responsa-bilidad	Referencia	Evaluación EC/EP/NE	Documentar
		aplicado sobre el centro de datos principal.	tecnológica			

El paso 10 del procedimiento para restablecer a las condiciones normales descritos en la Tabla 20 de esta guía, se ejecutará de manera exclusiva para el Servidor de Dominio.

Este procedimiento para restablecer a las condiciones normales puede ser utilizado para recuperar los otros servidores críticos en el sitio principal, sólo que debemos considerar la no ejecución del paso 10 para estos otros servidores.

El orden de recuperación de estos servidores en el sitio principal es el que describimos a continuación:

1. Servidor de Red.
2. Servidor del Sistema de Crédito.
3. Servidor de Correo electrónico.
4. Servidor del Sistema de Planillas y Cheques, y su unidad de almacenamiento (SAN). Para instalar el SAN en el sitio alterno, se depende de los conocimientos del proveedor (DELL), para lo cual

debemos utilizar el Anexo E (Proveedores Externos) para localizarlo y que procedan con la instalación y restauración de este equipo. Por lo cual existe dependencia del proveedor.

5. Servidor de Becas.
6. Servidor del Sistema de Imágenes.

Cuando se encuentren instalados y configurados los equipos críticos en el sitio principal, se debe proceder con la otra parte del Plan de Recuperación de Desastres de las Aplicaciones y Bases de Datos la cual se encuentra desarrollada en otro documento o guía para este fin.

4.6 PROCEDIMIENTO PARA EVALUAR EL DRP.

Según Cobit, en su DS4, Asegurar el Servicio Continuo. Cuando se efectúe una exitosa o fallida reanudación de la función de TI después de un desastre, la Dirección de Tecnología Informática del IFARHU deberá establecer procedimientos para evaluar lo adecuado del plan y actualizarlo de acuerdo con los resultados de dicha evaluación.

Se debe contar con un plan de pruebas a realizar al DRP buscando con esto mejorar los procesos de recuperación, documentar los resultados de la pruebas, actualizarlos y cumplir con los tiempos definidos en Análisis de Impacto del Negocio (BIA).

Para contar con un procedimiento de evaluación del DRP nos apoyamos en el Procedimiento General de Recuperación definido en la Tabla 18. Las columnas "Evaluación EC/EP/NE" (donde EC= Ejecución Completa, EP = Ejecución Parcial o falta completar el procedimiento y NE = No se Ejecutó el procedimiento). Esta columna de la Tabla 18 corresponde a la comprobación de estado de dicha acción o procedimiento, también contamos con la columna de Documentar, donde se describirá por qué la acción se ejecutó parcialmente (EP) o no se ejecutó (NE).

Como procedimiento para evaluar el Plan de Recuperación de Desastres del IFARHU tenemos el siguiente:

1. En la medida que cada una de las acciones se esté ejecutando, el Asesor en seguridad debe llenar las columnas del procedimiento donde se indica si la acción se ejecutó de manera competa, parcial o no se ejecutó.
2. El Asesor en seguridad deberá documentar cual fue la falla o el percance que motivó a que la acción fuese ejecutada parcialmente o por qué no se ejecutó, esto

lo hace en la columna Documentar del Procedimiento General de Recuperación descrito en la Tabla 18 de este documento

3 Una vez terminado el proceso de recuperacion y de retorno al sitio primario el Asesore de Seguridad debera entregar al Director de Tecnologia del IFARHU el procedimiento denominado Plan General de Recuperación con la información de la evaluación y la documentacion

4 El Director de Tecnologia dentro de los 10 dias hábiles posteriores a la reanudación de las operaciones de TI en el sitio principal convocara a reuniones al comité de evaluación del DRP para evaluar los resultados y tomar las acciones pertinentes para mejorar o actualizar el plan

5 Una vez hechas estas evaluaciones son pasadas al comité de mantenimiento del DRP para que las actualice

6 Luego de actualizadas por el comite de mantenimiento del DRP este lo envie al Comite de Distribución del Pan de Recuperación de Desastres para que sea distribuido al personal encargado de ejecutar el mismo

Este procedimiento debe ser utilizado tanto para cuando se realicen pruebas al DRP como cuando se origine una catástrofe que afecte los servicios criticos del centro de cómputo del IFARHU

CONCLUSIONES

La utilización de frase "espere lo mejor, pero prepárese para lo peor"[25] nos resume la parte esencial de un plan de recuperación en caso de desastre.

Una de las principales estrategias que deben tener las organizaciones modernas es tener dentro de sus planes estratégicos la continuidad del negocio como uno de sus objetivos principales.

Por lo anterior concluimos que dentro de la gestión de Tecnología de la Información, la continuidad de los servicios es considerada una parte esencial, razón por la cual el contar con un Plan de Recuperación de Desastres que garantice la continuidad de las operaciones en los tiempos definidos en el Análisis de Impacto del Negocio, es fundamental en toda organización que cuente con un centro de cómputo que brinde servicios a sus clientes y usuarios a través de los equipos y sistemas alojados en él.

Lo anterior nos ha llevado a desarrollar una guía para que sea utilizada en una institución estatal de Panamá, el Instituto para la Formación y Aprovechamiento de los Recursos Humanos (IFARHU), entidad esta que cuenta con un centro de cómputo a través del cual se ofrecen una serie de servicios.

La mejor manera para el desarrollo de esta guía fue utilizar metodologías o estándares internacionales como COBIT, ITIL, NIST, BCI, ISO, etc, especializadas en continuidad

[25] Proverbio Ruso, significa que nunca esperas que algo pase y si pasa debes estar preparado.

de servicios además fue de gran ayuda las entrevistas que se realizaron al personal directivo de la institución los cuales con su experiencia en el manejo de los servicios contribuyeron y aportaron sus valiosos conocimientos que nos ayudaron a identificar los procesos criticos de la institución y por ende identificamos los equipos criticos otro aspecto valioso en las entrevistas fue la del desarrollo del Análisis de Impacto del Negocio (BIA) que combinados con las metodologias utilizadas nos llevaron al desarrollo de este documento

Fue de gran importancia que la Dirección de Tecnologia Informática del IFARHU contara con los procedimientos actualizados de instalacion recuperación respaldo etc de los equipos criticos del centro de cómputo lo cual nos ayudó a la consecución del procedimiento general de recuperación y el de restablecimiento de las operaciones en el sitio principal

Lo ideal para el IFARHU en contar con un sitio alterno donde se encuentren instalados los equipos que se utilizarán para el DRP y sobre todo una vez se utilice esta guia para la implementacion del Plan de Recuperación de Desastres se deben realizar pruebas periódicas (minima una al año) donde se evalua la efectividad del plan

Con estas pruebas se deben llevar un control documentado de la efectividad de los procedimientos utilizados para asi poder utilizar esta documentación en la actualización constante de dicho plan con lo anterior obtendremos una mejora continua en el DRP

Y por ultimo cada vez que el plan se actualice debe existir una distribucion de la ultima versión probada entre las personas encargadas de ejecutar el plan y ademas de mantenerla en el sitio alterno de recuperación

RECOMENDACIONES

Estas recomendaciones están dirigidas a Dirección de tecnología del IFARHU, con miras a hacer más eficiente la guía para el desarrollo y aplicación del DRP.

- Realizar mínimo una prueba anual al DRP, (recomendable dos al año) o cuando se den cambios importantes en la infraestructura técnica de los equipos críticos.
- Es esencial contar con el apoyo y soporte de la alta dirección del IFARHU, quienes deben participar como patrocinadores del DRP tomando decisiones de manera proactiva.
- Es necesario integrar una gran parte de la institución con una participación activa, ya sea como parte del equipo del proyecto o como ejecutores de los procedimientos.
- Mantener activos en la institución los comités que forman parte de la Administración del Plan, haciéndoles partícipes de las pruebas que se realicen al mismo.(Comité de Distribución, de Entrenamiento, Pruebas y Mantenimiento)
- Mantener actualizados con las últimas versiones de sistemas operativos y configuraciones los equipos y sistemas críticos del centro de cómputo del IFARHU así como los de su centro alterno de recuperación.
- Contratar de manera permanente al Asesor en Seguridad Informática para que forme parte de la Dirección de Tecnología Informática de la institución y que su nivel de pertenencia y apego esté más comprometido.

- Como el desarrollo de este tipo de proyecto y su mantenimiento constante absorbe mucho tiempo se recomienda contratar personal exclusivo para estos fines
- La Direccion de Tecnologia debe asegurar la continuidad de las operaciones razón por la cual es imprescindible que el personal que participe del plan se encuentre entrenado en la ejecución del mismo y en el restablecimiento a las condiciones normales después de la contingencia
- La dirección de Tecnologia debe asegurar mantener actualizados todos los procedimientos utilizados en el DRP
- Mantener actualizado el Analisis de Impacto del Negocio ya que en este se definen el RPO RTO y MTD utilizados para el desarrollo de esta guia
- Mantener los contratos de terceros de Tecnologia actualizados con los niveles de servicios (SLA) apropiados ya que son parte esencial en el DRP
- En dado caso recomendamos la utilización de una empresa especializada en brindar el servicio de sitio alterno para recuperacion de desastres
- La ubicación de este sitio alterno debe estar localizado lejos del sitio principal preferiblemente en otro pais
- Los datos sistemas y aplicaciones deben estar instaladas en el sitio alterno de tal manera que la guia para la implementación del DRP se concentre en el levantamiento y ejecucion del mismo
- Es recomendable para actualizar esta guia contemplar en un tiempo no mayor de un año con una herramienta de replicacion de los datos con lo cual reducimos los

tiempos de recuperación y mejoramos la eficiencia de la continuidad de las operaciones

GLOSARIO DE TÉRMINOS

AIG: Autoridad para la Innovación Gubernamental.

ASE: Asesor de Seguridad.

Backups: es una copia de seguridad de datos e información en un dispositivo para tal fin.

BIA: Análisis de impacto del negocio. Siglas en inglés: Business Impact Analysis.

BCI: Instituto de Continuidad del Negocio. Siglas en inglés: Business Continuity Institute.

CD: Disco compacto utilizado para almacenar información. Siglas en inglés: Compact Disk.

COBIT: Objetivos de Control para la Información y Tecnologías relacionadas. Siglas en inglés: Control Objectives for Information and related Technology.

DELL: DELL es una compañía multinacional estadounidense establecida en Round Rock (Texas) que desarrolla, fabrica, vende y da soporte a computadoras personales, servidores, switches de red, programas informáticos, periféricos y otros productos relacionados con la tecnología.

DRII: Siglas en inglés: Disaster Recovery Institute International.

DRP: Plan de Recuperación ante Desastres. Siglas en inglés: Disaster Recovery Plan.

Firewall: Sistema de seguridad para redes basado en reglas donde el tráfico de entrada y salida de los paquetes de datos debe pasar por un sistema que puede autorizar o denegar su paso, de acuerdo a las políticas de control de acceso entre redes.

ITIL: Biblioteca de Infraestructura de Tecnologías de Información. Siglas en inglés: Information Technology Infrastructure Library.

MTD: Tiempo máximo tolerable fuera de servicio. Siglas en inglés: Maximun Time Down.

NIST: Instituto Nacional de Estándares y Tecnología. Siglas en inglés: National Institute of Standards and Technology.

P09 Proceso de COBIT Evaluar y Administrar los riesgos de TI

Routers Es un dispositivo utilizado para enrutar paquetes entre redes además permite interconexión entre estas

RPO Punto de recuperación objetivo Siglas en inglés Recovery Point Objective

RTO Tiempo de recuperación objetivo después de un desastre Siglas en inglés Recovery Time Objective

Scripts Son conjuntos de instrucciones o comandos que permiten la automatizacion de tareas

SAN Es una red de área de almacenamiento Siglas en ingles Storage Area Network

Switches Son dispositivos digitales lógicos para la interconexion de redes de computadoras

USB Dispositivo de almacenamiento que utiliza una memoria flash para guardar información Siglas en inglés Universal Serial Bus

UPS Fuente ininterrumpida de poder Siglas en inglés Uninterruptible Power Supply

WRT Tiempo de trabajo en recuperación Siglas en ingles Work Recovery Time

REFERENCIAS BIBLIOGRÁFICAS

- Bajada, Stephen. ITIL Foundations. GTS Learning Group, 2007. p.irr.
- P.M.I. (Project Management Institute), Guía de los Fundamentos de la Dirección de Proyectos, PMBOOK Guide. Tercera Edición, Estados Unidos, 2004. p.irr.
- Wallace, M.; Webber, Lawrence. The Disaster Recovery Handbook: a step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets. [USA]: AMACOM, 2004.
- Gustin, J. Disaster & Recovery Planning: a guide for facility managers. (5th Edition) [USA]: The Fairmont Press, 2010.
- Gregory, P. IT Disaster Recovery Planning for Dummies. [USA]: Wiley Publishing, 2008.
- Pink Elephant, Fundamentos de ITIL V3, Cuaderno de Trabajo, Continuidad de Servicio, Burlinton Ontario, Julio 2010, p.p. 128-141
- [1] International Information Systems Security Certification Consortium, "Business Continuity and Disaster Recovery Planning", in The Official (ISC)2 CISSP CBK Review Seminar, Student Handbook, Version 12.0, Editorial High Stakes Writing, Massachusetts USA, 2011,pp II-1 – II-36.
- [2] Hiatt, Charlote. A Primer for Disaster Recovery Planning in a IT Environment. Published in the United States of America. Idea Group Publishing, 2000. p.irr
- [3]Departamento de Desarrollo Institucional, IFARHU "Manual de Organización y Funciones del IFARHU", Revisión 2012, Panamá. Online. Disponible en:

http://www.ifarhu.gob.pa/ifaweb/transparencia/Manual-2008_mef%20aprobado%207%20de%20abril.pdf

- [4] Departamento de Desarrollo de Sistemas, Dirección de Tecnología e Informática. Sitio Web del IFARHU. Derecho Reservado 2012, IFARHU. Online. Disponible en: http://www.ifarhu.gob.pa/ifaweb/Historia3.aspx
- [5] Portal en línea del IFARHU. Dirección de Tecnología e Informática. Sitio Web del IFARHU. Derecho Reservado 2012, IFARHU. Online. Disponible en: http://www.ifarhu.gob.pa/ifaweb/index.aspx
- [6]Autoridad Para la Innovación Gubernamental. Sitio Web de la AIG. Online. Disponible en: http://www.innovacion.gob.pa/acercade
- [7] Rengifo, F., Méndez, N., Méndez, M. (2007). Topologías más Comunes. Online. Disponible en: http://www.monografias.com/trabajos15/topologias-neural/topologias-neural.shtml
- [8] Nuria Espinosa Bustillo Senior Manager Systems & Process Assurance PricewaterhouseCoopers, Enrique Panadero Illera, Manager Systems & Process Assurance PricewaterhouseCoopers- CISA. La Necesidad de Implantación de un Plan de Continuidad del Negocio. Red de Seguridad. 2005. Editorial Borrmart. Online. Disponible en: http://www.borrmart.es/articulo_redseguridad.php?id=564
- [9] SISTESEG. Política de Continuidad del Negocio (BCP/DRP). Online. Documento PDF. Disponible en: http://www.sisteseg.com/files/Microsoft_Word_-_POLITICA_DE_CONTINUIDAD_DEL_NEGOCIO.pdf

- [10] Harris E. Sanahuja. Condiciones y Capacidades para la Reducción del Riesgo. Online. Disponible en: http://daraint.org/wp-content/uploads/2012/01/UTR_Panama.pdf
- [11] Debarati Guha-Sapir. (21 Dic. 2011). CredCrunch Newsletter, Issue No. 26, December 2011- "Disaster Data: A Balanced Perspective". Online. Disponible en: http://reliefweb.int/report/belize/credcrunch-newsletter-issue-no-26-december-2011-disaster-data-balanced-perspective%E2%80%9D
- [12] IT Governance Institute. (2007). COBIT PO 7.5 Dependencia sobre Individuos. Online. Documento PDF. Disponible en: http://cs.uns.edu.ar/~ece/auditoria/cobiT4.1spanish.pdf .Página 56.
- [13] Peña, José A. Cobit Aplicado para asegurar la Continuidad de las Operaciones. 4. Identificación de los procesos críticos y Análisis de Impacto al Negocio. Online. Disponible en: http://www.isacamty.org.mx/archivo/213-COBIT_Aplicado_Para_Asegurar_Continuidad_Operaciones.pdf
- [14]Leonardo Camelo. (2010, Mayo, 30). Análisis de Impacto de Negocios / Business Impact Analysis (BIA). [Online]. Disponible en: http://seguridadinformacioncolombia.blogspot.com/2010_05_01_archive.html
- J. León. (2012, Octubre 31). La Importancia de un DRP. [Online]. http://www.milenio.com/cdb/doc/impreso/9163135?quicktabs_1=1
- BS 25999-Part1: Business Continuity Management – Code of Practice. Online. Disponible en: http://www.zarifopoulos.com/files/BS-25999%20Business%20Continuity%20Certification_pending.pdf

- BS 25999-Part2: Business Continuity Management – Specification. Online. Disponible en: http://www.govchina.org/Soft/UploadSoft/201204/20120416081157777.pdf
- Marianne Swanson,Pauline Bowen, Amy Wohl Phillips, Dean Gallup David Lynes. (2010, Mayo).NIST Special Publication 800-34. Contingency Planning Guide for Federal Information Systems. Online. Disponible en: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf
- J.S. Villalobos. "Guía para crear un plan de recuperación en caso de desastre en el sistema informático del centro de datos de un grupo financiero". M.S. Tesis. Universidad para La Cooperación Internacional. San José, Costa Rica. 2008. Disponible en: http://www.uci.ac.cr/Biblioteca/Tesis/PFGMAP505.pdf

ANEXOS

ANEXO A - Directorio del Equipo de Recuperación de Desastres

Función		Rol	Posición	Nombre	Teléfono Celular	Teléfono Casa	Dirección
CRTI	**Coordinador**	Primario	Director de TI	Juan Pérez	66667777	3900000	Calle 6ta. Rio Abajo Casa H-110
		Secundario	Subdirector de TI	José Juárez	66788888	3901111	Edificio ABC, Avenida Balboa, Apartamento 8-C
CIT	**Coordinador**	Primario					
		Secundario					
	Servidores y HW	Primario					
		Secundario					
	Controlador de dominio	Primario					
		Secundario					
	Soporte Técnico	Primario					
		Secundario					
	Comunicaciones	Primario					
		Secundario					

Función		Rol	Posición	Nombre	Teléfono Celular	Teléfono Casa	Dirección
ASE	**Backup/Restore**	Primario					
		Secundario					
	Asesor de Seguridad	Primario					
		Secundario					

ANEXO B - Directorio de Servicios de Emergencia

No.	Empresa	Teléfonos
1	**SISTEMA NACIONAL DE PROTECCIÓN CIVIL (SINAPROC)**	*335
2	**COMPAÑÍA DE BOMBEROS**	
	Central de Emergencias	103
3	**POLICÍA NACIONAL**	104
4	**DEFENSA CIVIL**	
	Central de Emergencias	228-2187 *455
5	**AMBULANCIAS**	
	Alerta Medica	911
	Ambulancia	264-4122
	SEMM	366-0122
	EMI	236-6060
6	**IDAAN (Instituto de Acueductos y**	

No.	Empresa	Teléfonos
	Alcantarillados Nacionales)	
	Centro de Atención Ciudadana	311
7	**UNION FENOSA**	
		315-7222
	Contacto	800-8346

ANEXO C - Formato de Evaluación del Desastre

Descripción del Evento	
Fecha	/ / Hora : am/pm
Notificado por:	<indique el personal que notificó el evento>
Breve descripción del Evento:	<describa brevemente el evento>
Tipo de desastre:	<indique el tipo de desastre: Incendio, Terremoto, Sobre carga / falta de energía, Inundaciones, Huelgas, Falla en los sistemas ambientales, Mal tiempo>
Daño ocasionado:	<describa el daño ocasionado a la infraestructura e instalaciones>
Tiempo requerido para reparación:	<indique el tiempo requerido para completar la reparación> <En caso el tiempo requerido para completar la reparación de los daños sea mayor al tiempo de recuperación

	requerido por el negocio, se declara la situación de emergencia>
Locación de los puntos de encuentro	
Sitio de Recuperación de TI	<indique el sitio donde se procederá a recuperar el centro de datos>
Declaración del desastre	
Fecha	/ / hora : am/pm
	_____ _____ <colocar los nombres y firmas de las persona que declaran el desastre para proceder a operar en contingencia>
Autorizado por	

ANEXO D - Requisitos en el Centro de Datos Alterno

Los controles mencionados depende del contrato que se tenga con el proveedor (en caso el centro de contingencia sea albergado en un tercero). Así mismo se debe revisar que los servidores, servicios de contingencia y librerías de backup estén operando.

No	Requisito	S/N
Controles Generales		
1	Detectores de Humo	
2	Sensores de Temperatura	
3	Extinguidores (Tipo A/B/C/D)	
4	FM200	
5	Switch de corte de energia	
6	Detector de aniego	
7	Fuente de alimentación de energía externa	
8	Aire acondicionado (requerimientos mínimos de BTU)	
9	Falso piso / techo	

10	Cableado debidamente etiquetado bajo el falso piso	
11	Rack para servidores (con llave)	
Monitoreo de Seguridad Física		
1	Cámaras de vigilancia	
2	Controles Biométricos	
3	Sensores de Movimiento	
Controles para Contingencia		
1	UPS	
2	Planta Eléctrica	

ANEXO E - Directorio de Proveedores externos de mantenimiento de Equipos

Empresa	Servicio	Contacto	Teléfono Fijo	Celular	Dirección
	Servicio de mantenimiento preventivo y correctivo de servidores DELL				
	Servicio de Soporte y Mantenimientos de Equipos de Comunicaciones.				
	Servicio de Mantenimiento del Firewall.				
	Servicio de soporte de comunicaciones.				
	Servicio de unidades de				

	Almacenamiento				
	Servicio de mantenimiento preventivo y correctivo de servidores HP				
	Empresa encargada de Custodia de Cintas de backup				

ANEXO F - Reporte de Equipos Evaluados.

Nombre del equipo	Código del equipo	Estado
<indicar el nombre del equipo evaluado>	<indicar el código del equipo>	**<Indicar si el equipo evaluado se debe recuperar, comprar o arreglar>**

<En caso de tener que realizarse compras de equipos producto de la evaluación debe adjuntarse este anexo al informe de compra>

Fecha: <indicar fecha de evaluación>

Evaluador: <indicar nombre de las persona que evaluó los equipos>