UNIVERSIDAD APEC (UNAPEC)

DECANATO DE INGENIERÍA E INFORMÁTICA

ESCUELA DE INFORMÁTICA

Plan de recuperación ante desastres aplicado al área de tecnología del Ministerio de Educación de la República Dominicana (MINERD) en el periodo Enero-Abril 2012.

Sustentantes:

Gregorys José Sosa González	2006-0576
Jhancarlo Veras Chalas	2006-1486
Yamayco Sánchez Núñez	2007-0155

Asesores:

Ramón Gómez

Antonio Calderón

Monografía para Optar por el Título de:

Ingeniero en Sistemas de Información

Santo domingo, D.N. República Dominicana

Abril 2012

PLAN DE RECUPERACIÓN ANTE DESASTRES APLICADO AL ÁREA DE TECNOLOGÍA DEL MINISTERIO DE EDUCACIÓN DE LA REPÚBLICA DOMINICANA (MINERD) EN EL PERIODO ENERO-ABRIL 2012.

DEDICATORIAS

A Dios primeramente por su fortaleza cada vez que de rodillas conversaba con Él, porque me contestó muchas oraciones demostrándome que si me apoyaba, porque esta carrera fue una petición y me ha sido contestada.

A mi padre José Sosa porque aun hasta hoy cree en mí, porque su amor y apoyo es mi inspiración hasta el día de hoy.

A Josefa González, abuela y madre al mismo tiempo. No tengo palabras para expresar lo tanto que te he amado desde mi razón de ser y uso de conciencia, porque todos estos años has luchado para que sea lo que soy y que no me detenga jamás.

A mí siempre amada Yaneury Feliz que siempre cree en mí y está conmigo en cualquiera de las situaciones. Tu amor en estos años ha sido el más importante soporte para que pueda mirar hacia el futuro construyendo este presente.

Gregorys José Sosa González.-

A mi padre Santiago Veras Mejía por enseñarme durante su tiempo de vida que se debe de luchar y trabajar duro con dedicación y empeño para lograr lo que se quiere, además de ser probablemente la persona que más confió en mis habilidades y condiciones.

A mi bujía inspiradora, ejemplo y mi más grande orgullo, mi madre Thelma Celeste Chalas quien siempre me brinda todo su apoyo en mis proyectos y con una palabra de alivio y calma me provee el más bien intencionado de los consejos.

A mis hermanas Thelma Yannirys Montás Chalas, Alexandra Veras Chalas y Clarissa Veras Chalas quienes aunque no lo crean son parte esencial en mi vida y ocupan un lugar especial en mi corazón.

A mí amada y adorada novia Yemerlin Desiree Santos Peñaló quien en todo momento me demuestra su apoyo y comprensión de forma incondicional en los diferentes escenarios de mi vida.

Jhancarlo Veras Chalas.-

A Dios todopoderoso por haberme dado la salud, la fuerza y la sabiduría necesaria para concluir este trabajo de grado.

A mi madre Marta Núñez de Dios, y a mi tía Témpora Sánchez Lebrón, porque con su amor, dedicación y su apoyo incondicional han sido parte fundamental de mi inspiración.

A mi padre Tomas Sánchez, a mi padrastro Manuel Enrique Santana, mis hermanos Gladys Esther Sánchez, Oscar Andrés Santana, Laura Nicole Santana y demás familiares por ser partes tan importante en mi vida y brindarme su apoyo incondicionalmente. A mi hermana Gladys Esther te quiero dedicar estas líneas porque tú siempre has confiado en mí y mereces parte especial de todos mis logros.

A mi amada y futura esposa Yocely Rodríguez Sánchez por siempre creer en mí, amarme y apoyarme en todo los momentos difíciles.

Yamayco Sánchez Núñez.-

AGRADECIMIENTOS

Agradezco a Juan Pablo Noboa por su entera disposición y por abrir las puertas de la DGTIC dentro del marco de lo posible y que pudiéramos realizar este trabajo.

Agradezco a Abel Herrera porque aportó con dos valiosísimos libros que fueron la base de este trabajo prácticamente.

Agradezco a Yamayco Sánchez y Jhancarlo Veras, quiénes gracias a sus aportes profesionales a este trabajo se pudo moldear de la manera correcta. Sin sus críticas y continuas dudas este trabajo no ofreciera la calidad que contiene.

Gregorys José Sosa González.-

Agradezco al ser divino “Dios”, que representa el orden natural de las cosas por ser referencia de admiración, maravilla y reverencia para mi persona.

A mis compañeros en este trabajo de grado: Gregory Sosa y Yamayco Sánchez, por su empeño, dedicación y compromiso para la realización del mismo.

A los ingenieros: Edgar Morrobert, Enrique Gil y Carlos Berrios por sacar tiempo de sus ocupadas agendas y con sus experiencias, apoyo y consejos ser de gran utilidad para la realización de este trabajo de grado.

A Manuel Soto Peralta quien siempre nos mostró su apoyo y disponibilidad desde su posición de encargado de salas de internet en la biblioteca de UNAPEC.

Jhancarlo Veras Chalas.-

A Dios todopoderoso “Bienaventurado el hombre que halla la sabiduría, y que obtiene la inteligencia; porque su ganancia es mejor que la ganancia de la plata, y sus frutos más que el oro fino (Proverbios 3:13-14)”.

A mis amigos y compañeros del trabajo de grado Jhancarlo Veras, Gregorys Sosa por su apoyo, dedicación y esfuerzo para completar este trabajo de grado. A Jhancarlo Veras le dedico estas líneas extras porque más que mi amigo, mi hermano y futuro compadre, espero que siempre seamos como hermanos.

A mis amigos Carlos Manuel Báez, Wilkys Rodríguez y demás amigos por apoyarme en los buenos y malos momentos.

A los ingenieros: Edgar Morrobert, Enrique Gil, Dayner Feliz, y Leónidas López por dedicar parte de su tiempo en transmitir sus experiencias e ideales.

A Manuel Soto por su empeño y dedicación en ayudarnos con las aulas de la biblioteca.

Yamayco Sánchez Núñez.-

INDICE

RESUMEN

En el mundo de hoy, los sistemas de información forman parte fundamental de las organizaciones sin importar la actividad a la que estas se dediquen. Esto ligado a los constantes cambios climáticos a nivel global, impulsa la necesidad de contar con un Plan de Recuperación ante Desastres para evitar o reducir las pérdidas humanas, financieras y tecnológicas.

En el trabajo de grado presentado a continuación se elaboró un Plan de Recuperación ante Desastres (DRP) para el Ministerio de Educación de República Dominica (MINERD). Dicho trabajo investigó una herramienta que permita una preparación para posibles eventualidades o desastres, sean estas de origen humano o natural.

Además, se examinó la organización y su entorno tecnológico, los riesgos, procesos más importantes y los sistemas que los soportan. En ese mismo orden, se desarrolló una solución para recuperar los sistemas y los procesos críticos, se fomentó la capacitación en el tema de DRP en la organización y se indicó como se deben de manejar todas las instancias o equipos al momento de un evento.

INTRODUCCION

Este trabajo de grado se realiza con el objetivo ó propósito de obtener el título de Ingeniero en Sistemas de Información y al mismo tiempo, se pretende realizar un aporte significativo para el Ministerio de Educación de República Dominicana (MINERD).

En la actualidad el MINERD no cuenta con los debidos procedimientos o procesos para dar respuesta a la ocurrencia de desastres o eventos no programados. Esto hace necesario la elaboración de un Plan de Recuperación ante Desastres (DRP) que permita realizar un análisis de los riesgos actuales y sus posibles controles, la evaluación de los procesos organizacionales claves que son soportados por los sistemas de información, las posibles estrategias para recuperar las actividades u operaciones, las técnicas prácticas para recuperar los sistemas de información, un plan pruebas y mantenimiento del DRP, etc.

Con la aplicación del Plan de Recuperación ante Desastre (DRP) planteado en este trabajo el MINERD podrá contar con un conjunto de procedimientos de respuesta altamente efectivos que garantizarán la reducción del nivel de exposición al riesgo, permite la continuidad de sus actividades u operaciones, del cuidado de su personal, del cuidado de su imagen y reputación como institución, de la integridad de su información, la elaboración de programas de concientización y capacitación y por último, obtiene un plan de manejo de

incidentes y crisis para evitar el desasosiego tanto del personal de menor nivel como la gerencia o dirección de la institución.

El trabajo presentará la siguiente estructura con el objetivo de lograr el mayor entendimiento y establecer la secuencia de actividades correctas:

Capítulo I Información Institucional. En este capítulo se presentan las informaciones generales de la institución como son Visión, Misión, etc. También se presentan las informaciones de la DGTIC abarcando desde su Visión hasta la descripción del entorno tecnológico.

Capítulo II Conceptos Generales. En este capítulo se definen y estudian los conceptos generales que pueden ser de utilidad durante el trabajo de grado.

Capitulo III Evaluación de Riesgos. En este capítulo se identificarán los riesgos y controles, la probabilidad de ocurrencia y los activos de información de la DGTIC.

Capitulo IV Análisis De Impacto Del Negocio (BIA). En este capítulo se procederá a evaluar los procesos u actividades críticas para el MINERD y los sistemas que soportan estos.

Capítulo V Estrategias De Recuperación. En este capítulo se presentarán las estrategias más viables de acuerdo a los datos obtenidos en los capítulos **III** y **IV.**

Capítulo VI Desarrollo Del Plan De Recuperación Ante Desastres. En este capítulo se presentarán las acciones técnicas a realizar para poner en práctica la estrategia seleccionada en caso de la ocurrencia de un desastre.

Capítulo VII Diseño De Pruebas Y Mantenimiento Del Plan. En este capítulo se presentarán los tipos y periodos de pruebas a utilizar para el plan y la descripción de los procesos a realizar durante el mantenimiento.

Capítulo VIII Programa De Capacitación Y Concientización Del Plan. En este capítulo se presentarán las actividades o procesos a llevar acabo con el objetivo de lograr la capacitación y concientización del personal sobre un DRP.

Capítulo IX Plan De Comunicación Ante Incidentes Y Crisis. En este capítulo se presentarán las actividades a realizar para el correcto manejo de las actividades a realizar durante la ocurrencia de un desastre para evitar el incorrecto manejo de este.

Capítulo I
Información Institucional

1.1 Reseña Histórica del Ministerio de Educación de la República Dominicana (MINERD)

En el año 1844, la función educativa estuvo a cargo del Ministerio de Justicia e Instrucción Pública, suprimido mediante la Ley No. 79, del 28 de enero de 1931. Luego con la Ley No. 89 del 21 de febrero del mismo año, se asignaron las atribuciones relacionadas con la Instrucción Pública y las Bellas Artes a la Superintendencia General de Enseñanza. El 30 de noviembre de 1934 con la Ley 786, fue creada la Secretaría de Estado de Educación y Bellas Artes. De esta manera el término "Instrucción" dio paso a un término más abarcador, como es el de "Educación".

En 1965, mediante el Decreto No. 16 de fecha 4 de septiembre, le fueron transferidas a la Secretaría de Estado de Educación, las funciones relacionadas con Cultos, anteriormente adscritas a la Secretaría de Estado de Relaciones Exteriores, con lo cual asumió el nombre de Secretaría de Estado de Educación Bellas Artes y Cultos.

Con la promulgación de la Ley No. 66-97 de fecha 9 de abril de 1997, la Secretaría cambia nuevamente de nombre, adquiriendo el de Secretaría de Estado de Educación y Cultura, que luego le fue cambiado por Secretaría de Estado de Educación con la aprobación y promulgación de la Ley 41-00 de fecha 28 de junio del año 2000, que crea la Secretaría de Estado de Cultura y que transfiere la función Cultural a esa cartera. El Reglamento Orgánico de fecha 11 de agosto del 2000, es el que opera la Ley de Educación 66-97.

El Articulo 134 de la Constitución de la R. D. proclamada en fecha 26 de enero de 2010, declara como Ministerio a las oficinas del estado. Mediante el Decreto No. 56-10, de fecha 06 de febrero de 2010, queda establecido que las

secretarías de Estado pasaron a denominarse ministerio. Por lo cual, la Secretaría de Estado de Educación con este Decreto, cambio su denominación a Ministerio de Educación de la República Dominicana.

1.2 Misión

Regular el Sistema Educativo dominicano de conformidad con la Ley General de Educación No. 66-97, garantizando el derecho de todos los dominicanos y dominicanas a una educación de calidad, mediante la formación de hombres y mujeres libres, críticos y creativos; capaces de participar y construir una sociedad libre, democrática y participativa, justa y solidaria, aptos para cuestionarla en forma permanente; que combinen el trabajo productivo, el servicio comunitario y la formación humanística, científica y tecnológica con el disfrute del acervo cultural de la humanidad, con la participación e integración de los distintos sectores de la sociedad, a fin de contribuir al desarrollo nacional y al suyo propio.

1.3 Visión

Lograr que todos los dominicanos y dominicanas tengan acceso a una educación pertinente y de calidad, asumiendo como principio el respeto a la diversidad, fortaleciendo la identidad cultural; formando seres humanos para el ejercicio de una vida activa y democrática, generando actitudes innovadoras y cambios en la sociedad y garantizando una calidad educativa que asegure el desarrollo sostenible y la cultura de paz.

1.4 Valores

- Creatividad en todas sus manifestaciones
- Inteligencia en todas sus expresiones
- Valores éticos
- Respeto a la vida
- Respeto a los derechos fundamentales de la persona
- Solidaridad
- Justicia
- Respeto a la verdad
- Igualdad de derechos entre hombres y mujeres
- Respeto a las diferencias individuales
- Dignidad
- Valores cristianos
- Valores comunitarios
- Valores patrióticos, participativos y democráticos en la perspectiva de armonizar las necesidades colectivas con las individuales
- Respeto al principio de convivencia democrática
- Conciencia de identidad
- Convivencia pacífica y de comprensión entre los pueblos
- Valoración del medio ambiente
- Valores estéticos

1.5 Funciones

Según la Ley General Educación 66-97.

Art. 74.- Los sectores funcionales están constituidos de la manera siguiente:

El Órgano de Decisión Superior, lo constituye el Consejo Nacional de Educación;

El Órgano de Conducción Superior, lo constituye el Secretario(a) de Estado de Educación y Cultura y, por delegación, los Sub-Secretarios;

El Órgano de Planificación, está constituido por los servicios de Planificación y Desarrollo Educativo;

El Órgano de Asesoramiento Técnico, está conformado por una de las Subsecretarías y los servicios técnicos pedagógicos;

Los Órganos de Ejecución, están conformados esencialmente por los Organismos Regionales, los Organismos Distritales y los Centros Educativos;

El Órgano de Supervisión y Control, está conformado por los servicios de Supervisión y Evaluación;

El Órgano de Apoyo Administrativo, está conformado por una de las Subsecretarías;

Los Órganos de Descentralización, están conformados por los Institutos Descentralizados, por las Juntas Regionales, por las Juntas Distritales y las Juntas de Centros Educativos;

Los Órganos de Coordinación con la Comunidad, están conformados por las asociaciones de padres, madres, tutores y amigos de la escuela, por las fundaciones y patronatos vigentes y por otras instituciones representativas de la comunidad.

Art. 75.- La definición de la naturaleza de esos órganos, sus funciones, sus esferas de competencia y su estructura de desarrollo organizativo serán aprobados en los reglamentos que al respecto dictará el Consejo Nacional de Educación, salvo los que expresamente se señalen en esta Ley.

1.6 Objetivos y estrategias

Fomentar la educación como recurso esencial para el desarrollo individual y primordial para el desarrollo social.

Formar personas capaces de contribuir eficientemente al progreso del país, mediante la creación de una conciencia de nación y la estimulación de la capacidad productiva nacional.

Dotar de una educación apropiada, gratuita y equitativa a todos los dominicanos, sin exclusiones.

Proteger y orientar la utilización racional de los recursos naturales, la defensa de la calidad del medio ambiente y el equilibrio ecológico.

Fomentar la interacción entre la vida educativa y la vida de la comunidad, a fin de propiciar la apropiación de los conocimientos y técnicas, de acuerdo con el desarrollo biopsicosocial de los ciudadanos.

Proveer los recursos necesarios para el desarrollo exitoso de los planes educativos.

1.7 Area de tecnología: Dirección General de Tecnologías de Información y Comunicaciones (DGTIC).

1.7.1 Visión

Ser el apoyo estratégico en gestión de servicios tecnológicos para el efectivo logro de los objetivos planteados por el Ministerio de Educación de la República Dominicana (MINERD) utilizando mejores prácticas que aseguren la excelencia de los resultados.

1.7.2 Misión

Asesorar, formular, implementar, administrar y evaluar acciones estratégicas de Tecnologías de Información y Comunicación con la intención de asegurar el correcto aprovechamiento de los recursos e impactar de manera efectiva en el logro de las metas y objetivos contemplados en las Políticas de Educación.

1.7.3 Objetivos

- Generar estrategias de implementación de TIC orientadas a satisfacer las demandas planteadas en los objetivos estratégicos del MINERD.
- Asegurar la estabilidad, la gestión, el desarrollo y el correcto aprovechamiento de los recursos tecnológicos del MINERD.
- Gestionar los sistemas operacionales, administrativos y financieros, para garantizar resultados efectivos a favor de los objetivos estratégicos de la institución.

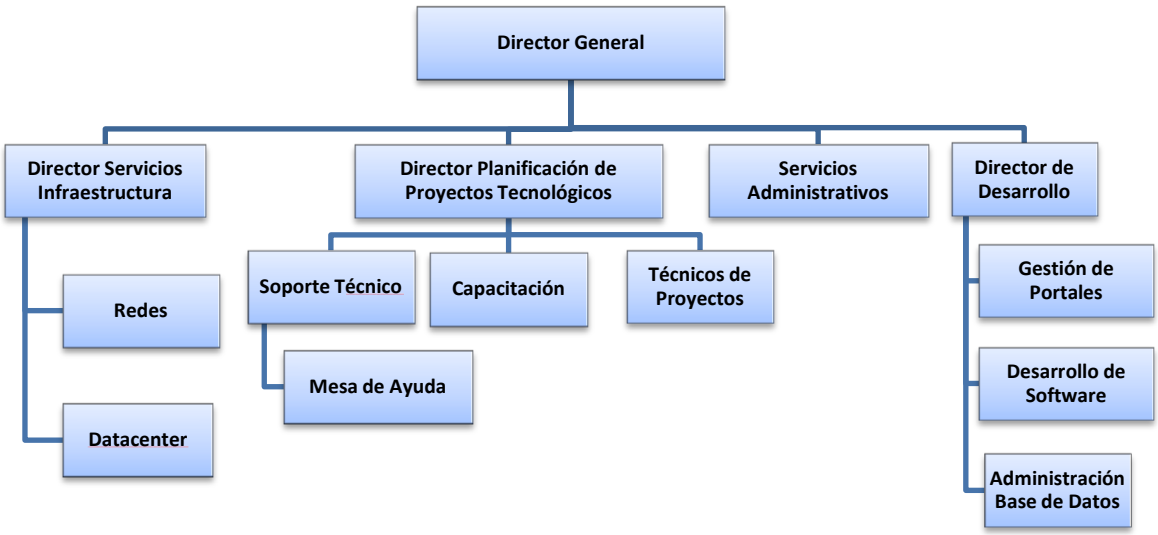
- Gestionar la conectividad, los sistemas de colaboración de información y los servicios de telefonía en toda la estructura del MINERD a nivel nacional.

1.7.4 Alcance

- Centros Educativos públicos.
- Distritos Escolares.
- Regionales Educativas.

1.7.5 Estructura de la Sede Central.

Compuesto por el director general, la estructura de la DGTIC tiene a su cargo cuatro directores de áreas imprescindibles para el funcionamiento de la dirección. A su vez, estos dirigen el resto de las áreas que soportan muchos de los procesos del MINERD. A continuación, el organigrama actual del DGTIC:



Fuente: Dirección General de Tecnología y Comunicación, 2010

1.7.6 Distribución del personal

Puestos	Cantidad
Directores	04
Coordinadores Técnicos	05
Especialistas	06
Técnicos Soporte	32
Auxiliares	26
Personal Mayordomía	03

1.7.7 Descripción del entorno tecnológico actual del DGTIC

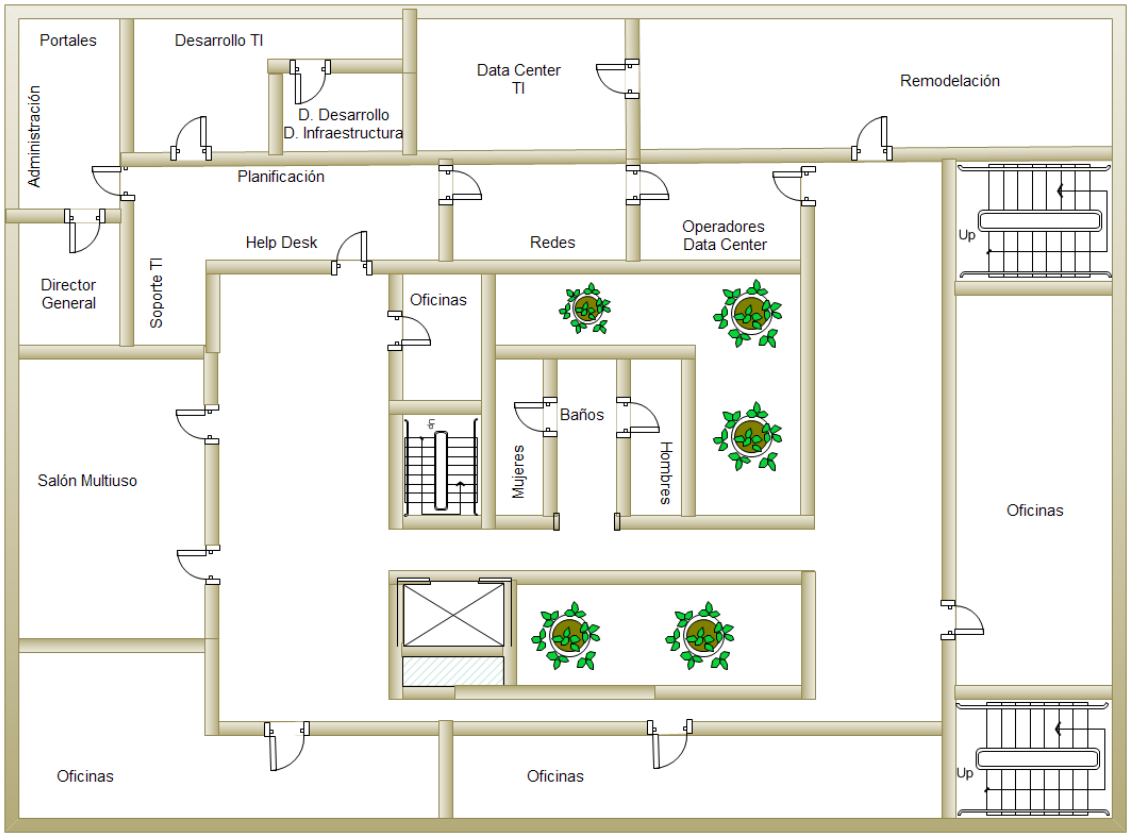
La estructura Informática actualmente soporta los servicios de aplicaciones, seguridad de data, conectividad y soporte técnico a las siguientes instancias:

Localidad		Usuarios	Computadoras
Sede Central SEE			
•Edif. Administrativo		1000	1000
•Edif. OCI		70	100
•Edif. Bienestar Estudiantil		90	40
•Edif. Pruebas Nacionales		30	30
•Radio Educativa		21	15
•Almacenes		6	9
	Total	***1217***	***1194***
•Regionales		270	110
•Distritos		630	530
	Total	***900***	***640***
•Centros Educativos			
•Administrativas		2500	2500
•Laboratorios			10 000
	Total	***2500***	***12500***
•INABIMA		15	10
•ISFODOSU			
•Administrativas		80	64
•Laboratorios			265
•IDEICE		100	25
	Total	***195***	***364***

Figura 1 – Fuente: Dirección General de Tecnología y Comunicación, 2010

Figura 2 - Fuente: Dirección General de Tecnología y Comunicación, 2010

A continuación se despliega un plano arquitectónico de las instalaciones físicas del 3er nivel que expone la DGTIC del MINERD por áreas:



Capítulo II
Conceptos Generales

2.1 Conceptos Básicos

Desastre: Desgracia grande, suceso infeliz y lamentable.

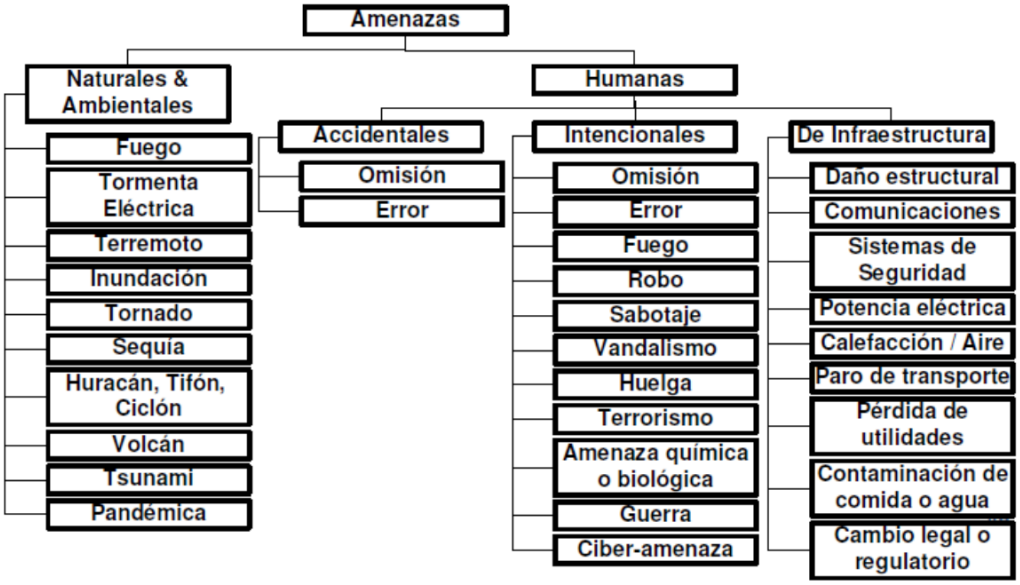
Centro de procesamiento datos (Datacenter): Es una ubicación en la cual se encuentran los recursos necesarios para el procesamiento de la información de una organización.

Infraestructura: Se refiere las instalaciones básicas y las facilidades en las cuales el crecimiento de la comunidad está confiado, como lo es plantas eléctricas, entre otros.

Amenaza: Cualquier circunstancia o evento con el potencial de impactar negativamente en las operaciones de la organización (incluyendo la misión, funciones, imagen o reputación), los activos de la organización o individuos a través de un sistema de información por medio del acceso no autorizado, destrucción, divulgación, modificación de la información, y / o denegación de servicio.

También se puede definir como cualquier cosa que puede causar o provocar daño o dolor a personas, animales u objetos. Estas pueden de ser de origen natural, animal y humanos, este último que a su vez puede ser intencional o no.

En el siguiente cuadro se presentan de forma detallada amenazas con su clasificación:



Vulnerabilidad: Característica o situación puntual de un activo u objeto que puede ser aprovechada o explotada por un amenaza. También puede decirse que es una cualidad que indica cierta sensibilidad ante la presencia de una amenaza.

2.2 Plan de Continuidad de Negocio (BCP)

El plan de continuidad de negocios (BCP) por sus siglas en inglés, maneja la capacidad de procesar los sistemas de negocio crítico en el momento de ruptura de las operaciones normales de procesamiento del mismo. La formulación del BCP involucra preparación, prueba y mantenimiento de acciones específicas para proteger los procesos críticos desde el efecto de la interrupción del servicio de procesamiento de datos[1].

[1] HANSCHE, Susan. BERTI, John. HARE, Chris. (2003). Official, (ISC)² Guide To The CISSP Exam. (pp. 663). Boca Raton, Florida. CRC, Press.

Las organizaciones escriben varios tipos de planes, como los Planes de Contingencia, Plan de Recuperación de Desastre (BCP), Planes de Reanudación (BRP), o el Plan de Recuperación de Desastres (DRP), que aseguran la disponibilidad de la información crítica en el momento de una inesperada interrupción causada por cualquier evento o desastre.

2.3 Plan de Recuperación ante Desastres (DRP)

Plan de recuperación de desastre se refiere a la inmediata y temporal restauración de los sistemas computacionales críticos y las operaciones con redes después de un desastre natural o alguna interrupción humana. Una organización documenta como va a responder ante un desastre y restaurar las funciones críticas de negocio dentro de un período de tiempo determinado; minimiza la pérdida y repara los daños dentro de la localidad para restituir el procesamiento de datos.[2]

El DRP se enfoca en la recuperación de los datos, las instalaciones físicas que albergan los servidores (Hardware), las aplicaciones o programas de computadores (Software) que sean críticos, para que las operaciones del negocio puedan ser recuperadas en el tiempo necesario en caso de cualquier evento no programado.

[2] HANSCHE, Susan. BERTI, John. HARE, Chris. (2003). Official, (ISC)² Guide To The CISSP Exam. (pp. 666). Boca Ratón, Florida. CRC, Press.

2.4 Ciclo de vida de un DRP

El ciclo de vida de un DRP se puede definir como un conjunto de fases que interrelacionadas persiguen asegurar la restauración o recuperación de los procesos tecnológicos que apoyan las operaciones de una organización ante la ocurrencia de cualquier desastre o evento no programado.

Las organizaciones sufren constantes cambios en sus procesos de negocios y tecnológicos siempre en busca de lograr una ventaja competitiva en el mercado en que se desenvuelven y mayor rentabilidad en sus operaciones. Dichos cambios obligan a mantener un constante monitoreo del Plan de Recuperación ante Desastres (DRP), debido a que por la falta de supervisión y actualización del mismo la organización puede provocar la no consecución de la recuperación total o parcial de sus sistemas de información sobre los cuales se apoyan los procesos críticos de la misma.

Algunos de estos cambios pueden ser:

- Cambios de personal o roles
- Cambios de activos de tecnología
- Cambios en el mercado
- Cambios estructurales o geográficos
- Cambios de negocios

En la siguiente imagen se muestran las fases o pasos del ciclo de vida de un DRP:

2.4.1 Análisis de Riesgos

El Análisis de Riesgos es una actividad que busca identificar las posibles vulnerabilidades, amenazas y la exposición de la organización hacia estas.

En esta parte se realiza una evaluación minuciosa y detallada de todo el entorno de la empresa o institución sobre todo del área de tecnología.

Algunos de los elementos o componentes a evaluar podrían ser:

- Ubicación geográfica
- Estructura
- Seguridad física
- Inventario de Software
- Inventario de Hardware
- Políticas de seguridad y accesos
- Entre otros.

2.4.2 Análisis De Impacto Al Negocio (BIA)

El Análisis de Impacto al Negocio es una actividad que busca identificar los procesos críticos del negocio sobre los cuales se apoya la organización para operar y el impacto que provocaría la salida de servicio o no disponibilidad de los procesos en caso de un desastre o evento no programado.

El BIA es el corazón del DRP dado que en base a este se obtiene el conocimiento de cuáles son los procesos prioritarios o de mayor importancia para la organización y además se diseñan las estrategias para la implementación del Plan de Desarrollo ante Desastres. Luego de identificados los procesos en el BIA la decisión final de cómo se ejecutará la recuperación respecto el orden queda a cargo de la gerencia de la organización.

En el Análisis de Impacto se deben tomar en consideración varios elementos entre los cuales están:

- Sistemas de información
- Dependencias entre procesos y sistemas
- Personal
- Suplidores
- Activos
- Procesos de negocio
- Acuerdos de niveles de servicios (SLA)
- Entre otros.

2.4.3 Estrategias De Recuperación

Las Estrategias de Recuperación buscan seleccionar las tácticas adecuadas para minimizar el impacto de un desastre o evento no programado si este ocurriera y afecta los procesos identificados y seleccionados anteriormente en el BIA.

Las estrategias de recuperación buscan conservar los procesos, servicios y sus dependencias en estado idóneo, el cual permita la utilización de estos en el menor tiempo posible.

2.4.4 Desarrollo De Plan

Esta actividad o conjunto de actividades se enfoca en la implementación y puesta en marcha del plan antes diseñado basado en las estrategias seleccionadas. En este se define como serán ejecutados los procedimientos para recuperar los sistemas que apoyan los procesos críticos antes identificados.

Para el Desarrollo del Plan se deberán de formar equipos los cuales serán responsables de diversas funciones entre las cuales se encuentran:

- Repuestas ante alertas
- Respuestas ante incidentes
- Procedimiento de transición
- Procedimiento de vuelta a normalidad
- Entre otros.

2.4.5 Pruebas y mantenimiento

El objetivo de esta fase es definir las pruebas a realizar del plan ya implementado. Esto abarca desde el tipo de pruebas a usar hasta el tiempo o periodo entre estas.

También se definen las siguientes cuestiones:

- Periodos de mantenimiento
- Revisión del plan con el objetivo de mantenerlo actualizado.
- Oportunidades de mejora
- Respuestas de los diferentes elementos del plan (Personal, sistemas, etc.)
- Entre otros.

2.5 Matriz RACI

Es una herramienta que permite identificar los roles y responsabilidades de las personas en el desarrollo de actividades y procesos. La matriz RACI define quién es la persona o grupo responsable de asegurar de realizar o ejecutar una función, así también, quién supervisa que se haga lo que se tiene que hacer y cómo se debe hacer solicitando además la rendición de cuentas a los responsables, a quien o quienes consultar para completar la función y a quien informar dentro de un marco de trabajo orgánico.

A continuación se indican cómo se designan los roles dentro de esta herramienta con una descripción resumida de su función:

- ***R*esponsible o <u>R</u>esponsable**

  Su función es realizar las actividades, tareas o procesos prácticos definidos.

- ***A*ccountable o <u>S</u>upervisor**

  Su función es supervisar o dar seguimiento a las actividades realizadas por los responsables ya antes designados.

- ***C*onsulted o <u>C</u>onsultado**

  Este rol representa a la persona o equipo de personas quienes serán consultados para completar la actividad. Este rol representa regularmente los miembros que más experiencia tienen respecto a un tema.

- ***I*nformed o <u>I</u>nformado**

  Este rol representa a la persona o equipo que deberán de ser informados durante y después de las actividades, tareas o procesos.

2.6 Definiciones de RTO, RPO y RTA

Objetivo de Tiempo de Recuperación (RTO): Es el periodo máximo de tiempo que un proceso de negocio puede estar fuera de servicio antes de ser reiniciado.

Objetivo de punto de recuperación (RPO): Es la cantidad máxima de pérdida de datos que una organización puede tolerar ante un desastre que interrumpa los procesos críticos del negocio.

Tiempo de Recuperación Actual (RTA): Es el periodo de tiempo que el soporte tecnológico puede recuperar la infraestructura del negocio.

2.7 Equipo de Respuesta en Emergencia

Equipo de respuesta en emergencia (ERT): Es el equipo de personas dentro de la organización que pueden ser contactadas a cualquier hora del día o de la noche, cuando ocurra un desastre.

Capitulo III
Evaluación de Riesgos

3.1 Definición de Evaluación Riesgos

La evaluación de riesgo es un tema que está estrechamente relacionado con los planes de continuidad de negocios y planes de recuperación de desastres. Este se define como la posibilidad de que se produzca un impacto determinado en la organización[3]. Simplemente esta evaluación calcula las vulnerabilidades y el impacto que se relacionan con los activos de la institución.

3.2 Riesgos Latentes para el MINERD

El término Riesgo Latente se refiere a la evaluación de las situaciones o circunstancias que podrían significar un posible peligro para la institución si se materializa una amenaza. Con esta evaluación se pretende lograr una identificación de las amenazas y vulnerabilidades de forma independiente, con el objetivo de entender las características que estas provocarían.

Luego de realizar las actividades antes indicadas se procederá con las recomendaciones o sugerencias de lugar para evitar que las amenazas aprovechen las vulnerabilidades y provoquen daños significativos a la organización.

3.2.1 Identificación de Amenaza y Vulnerabilidades

Antes de proceder con el desarrollo de este acápite sería de suma importancia recordar los conceptos de vulnerabilidad y amenaza.

[3]Jiménez, L. d. (2007). Guía de Desarrollo de un Plan de Continuidad de Negocios. Madrid, España: Escuela Universitaria de Informática, Universidad Politécnica de Madrid.

A continuación se presentan las amenazas consideradas con el objetivo de brindar entendimiento sobre cada una de estas y las vulnerabilidades asociadas a estas:

Huracanes. Son fenómenos naturales caracterizados por vientos de extraordinaria fuerza que oscilan entre 119 Km/h en su menor categoría y pueden llegar a superar los 250 Km/h en algunos casos. Estos además tienen giros en forma de torbellino y su diámetro crece a medida que avanzan apartándose de la zona donde se originan.

Los huracanes además de contar con las características antes mencionadas vienen acompañados en promedio entre $150mm^3$ y $300mm^{3.}$

Vulnerabilidad asociada: Una ventana abierta o sin protección.

Tormentas. Una tormenta es un disturbio atmosférico violento acompañado de un factor eléctrico y viento fuerte, lluvia, nieve o granizo. Los vientos de las tormentas son de menor intensidad que los huracanes pero que unidos a los demás factores pueden provocar destrucción.

Las tormentas pueden ser:

Eléctricas. Son fenómenos meteorológicos caracterizados por la presencia de rayos y sus efectos sonoros en la atmósfera terrestre denominados truenos.

Tropicales. Son fenómenos caracterizados por vientos circulares y con un centro de baja presión que arrastra agua en forma de lluvia.

Vulnerabilidad asociada: Falta de pararrayos, falta de tierra eléctrica en la edificación y falta de regulador o protección ante una variación de voltaje.

Incendio. Un incendio es una presentación de fuego no deseada que puede afectar un área libre o espacio natural, estructura física y a seres vivos. Este trae como resultado la fuerte conflagración de objeto u organismo que se exponga a este por un periodo de tiempo extenso.

Los incendios pueden clasificarse en:

Fuegos Fortuitos. Son aquellos fuegos que aparecen como resultado de un conjunto de fenómenos o condiciones de tipo natural entre las cuales podemos citar: Viento, humedad, deshidratación vegetal, emisiones de Etileno hacia la atmósfera, etc.

Fuegos Intencionados. Son aquellos que son originados por la mano humana con el propósito de provocar daño a un objeto, estructura o ser vivo. Entre las posibles razones de estos están: Venganzas personales, sabotaje, vandalismo, etc.

Vulnerabilidad asociada: Desperfectos en el cableado, poca protección de sistemas de detección y control de incendios fuera de funcionamiento.

Terremoto. Es una violenta sacudida de la corteza de la Tierra que puede provocar la destrucción de los edificios y los resultados de la liberación repentina de la tensión tectónica a lo largo de una línea de falla o de la actividad volcánica.

Vulnerabilidad asociada: El diseño y época de construcción.

Tsunami o Maremoto. Agitación violenta de las aguas del mar a consecuencia de una sacudida del fondo, que a veces se propaga hasta las costas y en algunos casos sobrepasa las mismas dando lugar a inundaciones.

Vulnerabilidad asociada: La cercanía a la costa.

Problemas de Climatización. Con problemas de climatización se entiende aquellas situaciones en las cuales se presentan condiciones inesperadas de temperatura en un área específica las cuales que podrían provocar daño.

Para la elaboración de este DRP se evaluarán las siguientes:

Humedad. Cantidad de vapor de agua que se encuentra en el aire.

Contaminantes peligrosos suspendidos en el aire. Estos pueden presentarse como material expulsado por dispositivos dentro del mismo centro de datos. Ejemplo: El hidrógeno de las baterías.

Vulnerabilidades asociadas: Falta de instalación de sensores de humedad, de químicos e hidrogeno y de polvo.

Variación Eléctrica. La variación eléctrica se refiere a las situaciones que abarcan todo cambio inesperado en la calidad y cantidad del flujo de electricidad.

Para la elaboración de este DRP se evaluarán las siguientes:

Alto voltaje. Que transmite o funciona con una diferencia de potencial entre los extremos de un conductor, o alto voltaje. También llamado alta tensión.

Bajo voltaje. Voltaje que según los estándares de ANSI/IEEE es de 1.000 voltios o inferior; los circuitos que operan con este tipo de voltaje no requieren una red de protección.

Ambas situaciones de presentarse pueden provocar serios daños a equipos y en casos extremos podrían provocar incendios, daños al personal, entre otros.

Vulnerabilidades asociadas: Falta de tierra eléctrica en la edificación, falta de regulador o protector ante una variación de voltaje.

Degradación del Hardware. Se entiende por Degradación del Hardware toda aquella situación que indique que los equipos y dispositivos utilizados no están aptos para el uso de los sistemas de información existentes.

Esta puede estar caracterizada por la obsolescencia respecto al sistema de información que se maneja en este así como también por la degradación en el desempeño o funcionalidades por el constante uso o la falta de mantenimiento.

Vulnerabilidad asociada: No contar con una política de mantenimiento y actualización de los equipos debidamente formada.

Incumplimientos Legales. El cumplimiento legal es una amenaza real dado que para ciertas plataformas. La no ejecución o consecución de un acuerdo de nivel de servicio (SLA) o la violación de los diferentes licenciamientos de sistemas de información manejados, pueden llevar a daños significativos que afectarían tanto los procesos como la imagen de la institución.

Vulnerabilidades asociadas: El no establecimiento de los acuerdos de niveles de servicio debidos, no contar con un debido inventario de sistemas de información.

Hacking. El Hacking son un conjunto de técnicas que tienen como objetivo el ingreso y violación a los sistemas de información sin autorización del afectado.

Algunas de las técnicas son:

Phishing. Consiste en el envío masivo de mensajes electrónicos que fingen ser notificaciones oficiales de entidades/empresas legítimas con el fin de obtener datos personales y bancarios de los usuarios.

Escaneo de Puertos. Consiste en detectar qué servicios posee activos un equipo para luego con la utilización de estos el atacante realiza alguna acción o daño.

Wardialers. Son herramientas de software que utilizan el acceso telefónico de una máquina para encontrar puntos de conexión en otros equipos o redes, con el objeto de lograr acceso o recabar información.

Software malicioso / Virus. Se define como todo programa o fragmento que genera algún tipo de problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con el funcionamiento normal.

Sniffing o Packet Sniffer. Es un software destinado para detectar tramas en la red. Estos tienen diversos usos como monitorear redes para detectar y analizar fallos o ingeniería inversa de protocolos de red, robar contraseñas, interceptar mensajes de correo electrónico, espiar conversaciones de chat, etc.

Desbordamiento de CAM. Se trata de inundar la tabla de direcciones de un Switch con el objeto de bloquear la capacidad que éste posee de direccionar cada paquete exclusivamente a su destino. De esta forma el atacante podrá efectuar Sniffing de los paquetes enviados por un Switch, cuando en condiciones normales un Switch no es vulnerable a este tipo de ataques.

Backdoors. Consisten en accesos no convencionales a los sistemas, los cuales pueden permitir efectuar acciones que no son permitidas por vías

normales. Generalmente son instalados por el atacante para lograr un permanente acceso al sistema.

Denegación de Servicio. Su objetivo es degradar considerablemente o detener el funcionamiento de un servicio ofrecido por un sistema o dispositivo de red.

Vulnerabilidades asociadas: Inyección de código SQL, falla en los controles de acceso, desactualización de los antivirus, vencimiento del licenciamiento, falta de monitoreo de las plataformas de telecomunicación.

Error humano y acceso del personal. Son aquellas acciones realizadas por el hombre de forma intencional o accidental. Entre estas acciones se encuentra el acceso no autorizado a áreas con intenciones dañinas.

Vulnerabilidades asociadas. Falta de instalación de sensores de rotura de vidrios, movimiento y vibración, falta de instalación de un sistema de cámaras.

3.2.2 Probabilidad De Ocurrencias De Riesgos

Todas las amenazas sin importar la naturaleza de las mismas se ven sujetas a ser valoradas según su probabilidad de ocurrencia, ¿Qué es una probabilidad?, una probabilidad se puede definir como el número de veces o frecuencia con la que un suceso u evento tiende a ocurrir o como una medida numérica que refleja la posibilidad de que ocurra un evento. Está permite obtener conclusiones sobre las características de la variable de una muestra o población. Definido y comprendido este término se realizará un análisis de la probabilidad de ocurrencia que tienen las amenazas más significativas que

podrían afectar el Ministerio de Educación de República Dominicana (MINERD).

A continuación se presenta un análisis de la probabilidad de ocurrencia de las amenazas identificadas en el acápite anterior:

Terremoto: Dado a que la Republica Dominicana o isla de la Hispaniola se encuentra ubicada en la placa Tectónica del Caribe; sus bordes contractan al norte con la placa de Norte América, al sur con la de Sudamérica, al oeste con la de Nazca y al este con el fondo Oceánico del Atlántico (ver figura 3). Esto

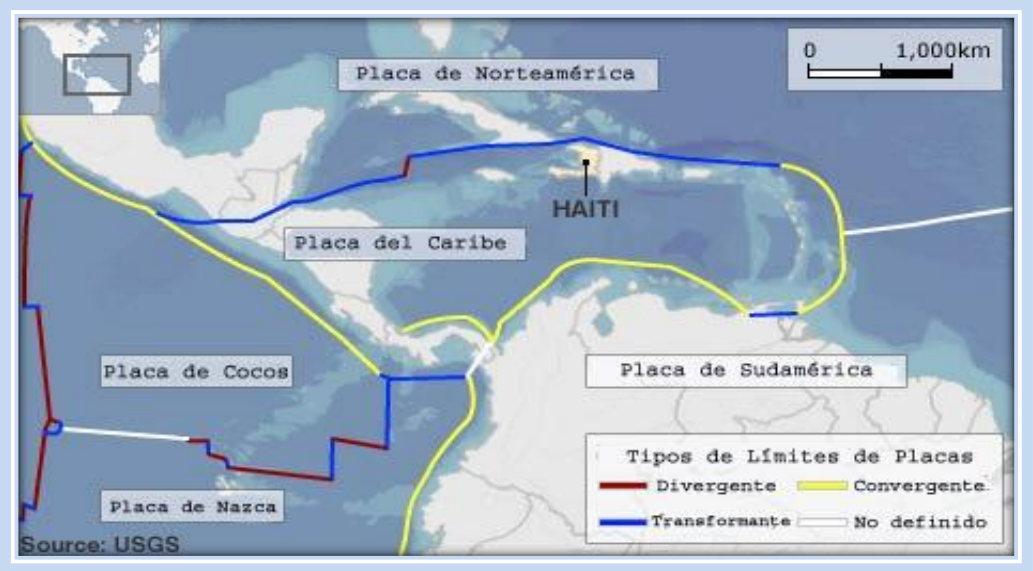


Figura 3

sumado a los datos extraídos del "Análisis de riesgo de desastres y vulnerabilidades de la Republica Dominicana" realizados en Marzo del 2009 el cual registra alrededor de 14 terremotos catastróficos en el país desde 1562 hasta la actualidad. Estas y otras razones hacen que el Ministerio de Educación de República Dominicana (MINERD), se encuentre con alta posibilidades de que en cualquier instante se vea afectado por un fenómeno de esta naturaleza.

A continuación se muestra la siguiente imagen (Figura 4) extraída el “Plan Nacional de Contingencia para Terremotos” realizado por COE en el 2009, en donde se presentan de formas detalladas las zonas de mayor exposición simiescas que tiene la isla.

Figura 4

Figura 5, **Fuente:** Análisis de riesgo de desastres y vulnerabilidades de la Republica Dominicana, Marzo del 2009

Tsunami o Maremoto: Pudiendo este ser generado por un movimiento telúrico dentro o fuera del lecho oceánico, sumado al análisis que se realizo sobre la probabilidad de ocurrencia de estos movimientos y compensado la cercanía que el MINERD tiene de la costa, esta se encuentra altamente amenazada.

Cabe señalar que los únicos eventos de esta naturalidad registrados en país datan del **11 de octubre de 1918 (Punta Cana)** y del **4 de agosto de 1946 (Nagua y Puerto Plata)** disipando la pérdida de un promedio de 501 personas registradas, lo que disminuye considerablemente el índice de ocurrencia de este tipo de catástrofe natural en nuestro país, aunque no reduce el daño que pudiera provocar la presencia del mismo.

Huracanes y Tormentas: La ubicación geográfica de la Republica Dominicana en la trayectoria de los huracanes y tormentas, sumado a la prolongada temporada a la que enfrentamos cada año, la cual comprende los meses de Junio-Noviembre, mantienen en constante amenaza el Ministerio de Educación de República Dominicana (MINERD). Analizando la cantidad de estos fenómenos que han ocurrido en las últimas décadas, hacen que la probabilidad de ocurrencia estos femémonos sea la más elevada. A continuación se muestra un mapa en donde se puede observar cuales son las zonas o provincias más amenazadas.

Figura 6, **Fuente:** Análisis de riesgo de desastres y vulnerabilidades de la Republica Dominicana, Marzo del 2009

Incendios: Los incendios son una de las amenazas más peligrosas y constante a la que se enfrenta cualquier institución, debido a que pueden ser provocados y propagados fácilmente por factores naturales o humanos. Para el MINERD su probabilidad de ocurrencia es bastante considerable dado a que en

la misma no existe un eficiente sistema de detección de incendio como se muestra en la imagen del anexo III.

Hacking: En los últimos años el crecimiento de esta amenaza técnica se ha elevado considerablemente tanto a nivel mundial como nacional. Ejemplo de esto es el ataque de denegación de servicio o DoS que recibió el Ministerio de Educación de República Dominicana (MINERD) el 22 de Agosto del 2011por el popular grupo de hacker anonymous.

Problema de Climatización: Los problemas de climatización son una amenaza que se debe considerar de forma especial en un centro de datos. Según aclaran Cristian Cowan y Chris Gaskins "A medida que los centros de datos evoluciona, y el procesamiento distribuido y las tecnologías para servidores elevan la demanda de energía y enfriamiento, se debe analizar el entorno más cuidadosamente "[4], estas y otras razones como son la cercanía al océano aumenta considerablemente la probabilidad de que el MINERD se vea afectado por un amenaza de esta naturalidad.

Error Humano y Acceso al Personal: Los errores humanos y acceso al personal son de alta frecuencia de ocurrencia en lugares en donde se carecen de controles o medidas de prevención para que no ocurran. Estos de ocurrir pueden provocar ceberos daños a los activos e imagen de la organización.

Inundaciones: Las inundaciones se convierten en una amenaza considerable debido a la alta frecuencia de ocurrencia de las mismas. Según un estudio realizado por la unión europea "A lo largo de los 35 años analizados, las

[4] COMO MONITOREAR LAS AMENAZAS FISICAS EN UN CENTRO DE DATOS. Consultado el 08 Marzo 2012. En la World Wide Web: http://www.fasor.com.sv/whitepapers/whitepapers/Monitoreo/Como_monitorear_amenazas_fisicas_en_centro_de_datos.pdf

inundaciones con mayor afectación en el país han presentado periodos de recurrencia de entre 4 y 6 años...”[5]. En la siguiente se muestran las provincias de mayor exposición a este fenómeno natural.

Figura 7, **Fuente:** Análisis de riesgo de desastres y vulnerabilidades de la Republica Dominicana, Marzo del 2009

Fallas Eléctricas: Las fallas eléctricas son una amenaza común para cualquier organización debido a que más de 90% de las operaciones de estas dependen de la electricidad. A esto se suma la inestabilidad del sistema eléctrico dominicano, lo que provoca que se eleven las probabilidades de ocurrencias.

3.2.3 Priorización De Riesgos

Para el proceso de priorización de riesgo se procederá a agrupar los activos en conceptos genéricos para que sea de mejor entendimiento y comprensión.

[5] ANÁLISIS DE RIESGOS DE DESASTRES Y VULNERABILIDADES EN LA REPÚBLICA DOMINICANA. Consultado el 08 Marzo 2012. En la World Wide Web: http://ec.europa.eu/echo/files/funding/opportunities/interest_dipecho7_Rep_Dominicana.pdf

- **Hardware TI.** Los activos identificados en esta categoría son:

  Computadores: escritorio (desktop) y portátiles (laptop)

  Enrutadores (Routers) y Conmutadores (Switch)

  Servidores

  Cableado UTP, fibra óptica

- **Sistemas de Información.** Los activos identificados en esta categoría:

  Bases de datos

  Aplicaciones Web y de escritorio

  Sistemas de firewall

  Sistemas Operativos

  Manejador de correo

- **Estructura física.** Los activos identificados en esta categoría son:

  Edificación y Mobiliario

- **Equipos Eléctricos.** Los activos identificados en esta categoría son:

  Planta Eléctrica

  UPS

  Cableado

A continuación se presenta la matriz de priorización de riesgo para un mayor entendimiento:

Ministerio de Educación República Dominicana (MINERD) **Matriz De Evaluación De Riesgo Enero-Abril 2012**							
Nivel de Impacto del Riesgo 1= Mínimo/5=Catastrófico; Probabilidad de Ocurrencia 1=Poco Probable/ 5= Muy Probable *Prioridad B=Baja/M=Moderada/A=Alta/E=Extrema*							
Activos	**Amenazas**	**Vulnerabilidad**	**Posibles Controles**	**Nivel de Impacto del Riesgo**	**Probabilidad de Ocurrencia**	**Medición de Riesgo**	**Prioridad**
Hardware TI.	Incendio.	Desperfectos en el cableado, poca protección de sistemas de detección y control de incendios fuera de funcionamiento.	Procurar la puesta en funcionamiento del sistema general de control de incendios, verificar el estado del cableado constantemente.	5	3	15	A
	Terremoto.	El diseño y época de construcción.	Reforzar la construcción de la estructura para acondicionarla a los nuevos tiempos y ante movimientos telúricos, instalación de plataformas anti sísmicas para los aparatos.	4	4	16	A
	Problemas de climatización.	Falta de instalación de sensores de humedad, de químicos e hidrogeno y de polvo.	Instalación de sensores de humedad, temperatura, polvo, hidrógeno.	3	2	6	B

Ministerio de Educación República Dominicana (MINERD) **Matriz De Evaluación De Riesgo Enero-Abril 2012**							
Nivel de Impacto del Riesgo 1= Mínimo/5=Catastrófico; Probabilidad de Ocurrencia 1=Poco Probable/ 5= Muy Probable *Prioridad B=Baja/M=Moderada/A=Alta/E=Extrema*							
Activos	**Amenazas**	**Vulnerabilidad**	**Posibles Controles**	**Nivel de Impacto del Riesgo**	**Probabilidad de Ocurrencia**	**Medición de Riesgo**	**Prioridad**
Hardware TI.	Variación Eléctrica.	Falta de tierra eléctrica en la edificación, falta de regulador o protector ante una variación de voltaje.	Instalación de tierras y reguladores de voltaje.	4	4	16	**A**
	Degradación del Hardware.	No contar con una política de mantenimiento y actualización de los equipos debidamente formada.	Desarrollar los procedimientos adecuados para monitorear constantemente el estado de los equipos, Roadmap para los equipos.	3	5	15	**A**
	Incumplimientos legales.	El no establecimiento de los acuerdos de niveles de servicio debidos, no contar con un debido inventario de sistemas de información.	Mantener una comunicación constante con todos los suplidores y asegurarse del diseño correcto de los SLA, supervisar los activos de los equipos incluyendo en estos las licencias.	3	3	9	**M**

Ministerio de Educación República Dominicana (MINERD) **Matriz De Evaluación De Riesgo Enero-Abril 2012**							
Nivel de Impacto del Riesgo 1= Mínimo/5=Catastrófico; Probabilidad de Ocurrencia 1=Poco Probable/ 5= Muy Probable *Prioridad B=Baja/M=Moderada/A=Alta/E=Extrema*							
Activos	**Amenazas**	**Vulnerabilidad**	**Posibles Controles**	**Nivel de Impacto del Riesgo**	**Probabilidad de Ocurrencia**	**Medición de Riesgo**	**Prioridad**
Hardware TI.	Tormenta.	Falta de para rayos, falta de tierra eléctrica en la edificación y falta de regulador o protección ante una variación de voltaje.	Instalar para rayos, instalar tierra eléctrica, protección contra variación de voltaje.	3	2	6	**B**
	Hacking.	Inyección de código SQL, falla en los controles de acceso, desactualización de los antivirus, falta de monitoreo de las plataformas de telecomunicación.	Establecimiento de un Sistema de Gestión de Seguridad Informática que abarque todas las plataformas y los controles.	4	4	16	**A**
	Error Humano y Acceso del Personal.	Falta de instalación de sensores de rotura de vidrios, movimiento y vibración, falta de instalación de un sistema de cámaras.	Reforzar los controles de seguridad, instalar sensores de rotura de vidrio, movimiento y vibración, cerciorarse de la instalación y correcto funcionamiento de un sistema de cámaras.	4	5	20	**E**

Ministerio de Educación República Dominicana (MINERD) **Matriz De Evaluación De Riesgo Enero-Abril 2012**							
Nivel de Impacto del Riesgo 1= Mínimo/5=Catastrófico; Probabilidad de Ocurrencia 1=Poco Probable/ 5= Muy Probable *Prioridad B=Baja/M=Moderada/A=Alta/E=Extrema*							
Activos	**Amenazas**	**Vulnerabilidad**	**Posibles Controles**	**Nivel de Impacto del Riesgo**	**Probabilidad de Ocurrencia**	**Medición de Riesgo**	**Prioridad**
Sistemas de Información.	Variación Eléctrica.	Falta de tierra eléctrica en la edificación, falta de regulador o protector ante una variación de voltaje.	Instalación de tierras y reguladores de voltaje.	4	4	16	**A**
	Degradación del Hardware.	No contar con una política de mantenimiento y actualización de los equipos debidamente formada.	Desarrollar los procedimientos adecuados para monitorear constantemente el estado de los equipos, Roadmap para los equipos.	2	5	10	**M**
	Incumplimientos legales.	El no establecimiento de los acuerdos de niveles de servicio debidos, no contar con un debido inventario de sistemas de información.	Mantener una comunicación constante con todos los suplidores y asegurarse del diseño correcto de los SLA, supervisar los activos de los equipos incluyendo en estos las licencias.	4	3	12	**M**

Ministerio de Educación República Dominicana (MINERD)
Matriz De Evaluación De Riesgo Enero-Abril 2012

Nivel de Impacto del Riesgo 1= Mínimo/5=Catastrófico; Probabilidad de Ocurrencia 1=Poco Probable/ 5= Muy Probable
Prioridad B=Baja/M=Moderada/A=Alta/E=Extrema

Activos	Amenazas	Vulnerabilidad	Posibles Controles	Nivel de Impacto del Riesgo	Probabilidad de Ocurrencia	Medición de Riesgo	Prioridad
Sistemas de Información.	Hacking.	Inyección de código SQL, falla en los controles de acceso, desactualización de los antivirus, vencimiento del licenciamiento, falta de monitoreo de las plataformas de telecomunicación.	Establecimiento de un Sistema de Gestión de Seguridad Informática que abarque todas las plataformas y los controles.	5	4	20	E
	Error Humano y Acceso del Personal.	Falta de instalación de sensores de rotura de vidrios, movimiento y vibración, falta de instalación de un sistema de cámaras.	Implementar controles y políticas de acceso a las aplicaciones y sistemas, cerciorarse que los sistemas tengan un diseño enfocado a evitar fallas humanas.	4	5	20	E
Estructura Física.	Huracanes.	Una ventana abierta o sin protección.	Reforzar la estructura para que esta sea más resistente a los vientos e inundaciones, instalación de sensores de rotura de cristales.	3	5	15	A

Ministerio de Educación República Dominicana (MINERD) **Matriz De Evaluación De Riesgo Enero-Abril 2012**							
Nivel de Impacto del Riesgo 1= Mínimo/5=Catastrófico; Probabilidad de Ocurrencia 1=Poco Probable/ 5= Muy Probable *Prioridad B=Baja/M=Moderada/A=Alta/E=Extrema*							
Activos	**Amenazas**	**Vulnerabilidad**	**Posibles Controles**	**Nivel de Impacto del Riesgo**	**Probabilidad de Ocurrencia**	**Medición de Riesgo**	**Prioridad**
Estructura Física.	Tormentas.	Falta de para rayos, falta de tierra eléctrica en la edificación y falta de regulador o protección ante una variación de voltaje.	Instalar para rayos, instalar tierra eléctrica, protección contra variación de voltaje.	3	3	9	**M**
	Incendio.	Desperfectos en el cableado, poca protección de sistemas de detección y control de incendios fuera de funcionamiento.	Procurar la puesta en funcionamiento del sistema general de control de incendios, verificar el estado del cableado constantemente.	5	3	15	**A**
	Terremoto.	El diseño y época de construcción.	Reforzar la construcción de la estructura para acondicionarla a los nuevos tiempos y ante movimientos telúricos.	4	4	16	**A**

Ministerio de Educación República Dominicana (MINERD) **Matriz De Evaluación De Riesgo Enero-Abril 2012**							
Nivel de Impacto del Riesgo 1= Mínimo/5=Catastrófico; Probabilidad de Ocurrencia 1=Poco Probable/ 5= Muy Probable *Prioridad B=Baja/M=Moderada/A=Alta/E=Extrema*							
Activos	**Amenazas**	**Vulnerabilidad**	**Posibles Controles**	**Nivel de Impacto del Riesgo**	**Probabilidad de Ocurrencia**	**Medición de Riesgo**	**Prioridad**
Estructura Física.	Tsunami o Maremoto.	La cercanía a la costa.	Diseñar una apropiada política de evacuación y protección para el personal y los equipos de ser posible.	5	2	10	**M**
	Variación Eléctrica.	Falta de tierra eléctrica en la edificación, falta de regulador o protector ante una variación de voltaje.	Instalación de tierras y reguladores de voltaje.	1	4	4	**B**
	Error Humano y Acceso del Personal.	Falta de instalación de sensores de rotura de vidrios, movimiento y vibración, falta de instalación de un sistema de cámaras.	Reforzar los controles de acceso a las diversas áreas y monitoreo del personal.	1	4	4	**B**
Equipos Eléctricos.	Huracanes.	Una ventana abierta o sin protección.	Reforzar la estructura para que esta sea más resistente a los vientos e inundaciones, instalación de sensores de rotura de cristales.	1	5	5	**B**

Ministerio de Educación República Dominicana (MINERD) **Matriz De Evaluación De Riesgo Enero-Abril 2012**							
Nivel de Impacto del Riesgo 1= Mínimo/5=Catastrófico; Probabilidad de Ocurrencia 1=Poco Probable/ 5= Muy Probable *Prioridad B=Baja/M=Moderada/A=Alta/E=Extrema*							
Activos	**Amenazas**	**Vulnerabilidad**	**Posibles Controles**	**Nivel de Impacto del Riesgo**	**Probabilidad de Ocurrencia**	**Medición de Riesgo**	**Prioridad**
Equipos Eléctricos.	Tormentas.	Falta de para rayos, falta de tierra eléctrica en la edificación y falta de regulador o protección ante una variación de voltaje.	Instalar para rayos, instalar tierra eléctrica, protección contra variación de voltaje.	5	3	15	A
	Incendio.	Desperfectos en el cableado, poca protección de sistemas de detección y control de incendios fuera de funcionamiento.	Procurar la puesta en funcionamiento del sistema general de control de incendios, verificar el estado del cableado constantemente, mantener un monitoreo constante.	5	3	15	A
	Terremoto.	El diseño y época de construcción.	Reforzar la construcción de la estructura para acondicionarla a los nuevos tiempos y ante movimientos telúricos.	4	4	16	A

Ministerio de Educación República Dominicana (MINERD) **Matriz De Evaluación De Riesgo Enero-Abril 2012**							
Nivel de Impacto del Riesgo 1= Mínimo/5=Catastrófico; Probabilidad de Ocurrencia 1=Poco Probable/ 5= Muy Probable *Prioridad B=Baja/M=Moderada/A=Alta/E=Extrema*							
Activos	**Amenazas**	**Vulnerabilidad**	**Posibles Controles**	**Nivel de Impacto del Riesgo**	**Probabilidad de Ocurrencia**	**Medición de Riesgo**	**Prioridad**
Equipos Eléctricos.	Tsunami o Maremoto.	La cercanía a la costa.	Diseñar una apropiada política de evacuación y protección para el personal y los equipos de ser posible.	4	2	8	**M**
	Problemas de climatización.	Falta de instalación de sensores de humedad, de químicos e hidrogeno y de polvo.	Instalación de sensores de humedad, temperatura, polvo, hidrógeno.	4	2	8	**M**
	Variación Eléctrica.	Falta de tierra eléctrica en la edificación, falta de regulador o protector ante una variación de voltaje.	Instalación de tierras y reguladores de voltaje.	5	4	20	**E**
	Error Humano y Acceso del Personal.	Falta de instalación de sensores de rotura de vidrios, movimiento y vibración, falta de instalación de un sistema de cámaras, falta de políticas en el manejo de líquidos.	Reforzar los controles de acceso a las diversas áreas y monitoreo del personal.	5	4	20	**E**

3.3 Proceso De Manejo De Riesgos

El proceso de manejo de riesgo es mediante el cual se tomaran las decisiones en un ambiente de indecisión sobre una acción que va a suceder y sobre el impacto que existiría si esta acción ocurriese. En el grafico mostrado a continuación se detallan los pasos que se deberán administrar para el manejo de los riesgos.

1. **Establecimiento De Contexto:** El establecimiento del contexto es la primera etapa a trabar en el proceso de manejo de riesgo, en donde es necesario identificar el ambiente organizacional en el que el riesgo se presenta. Para la identificación de estos riegos se debe de tomar en consideración las políticas, valores, objetivos y demás de la misma.

2. **Identificación De Riesgo:** Este es el segundo paso para el manejo de riesgo y consiste en identificar el riesgo observando todas las

perspectivas en que pudieran ocurrir. Para ello se utilizaran herramientas como son:

- Diagrama de flujo
- Técnicas de análisis de sistemas
- Entrevistas
- Discusiones en grupo y experiencia personal
- Inspección Física
- Otras.

3. **Análisis De Riesgo:** Esta es la tercera fase o etapa del proceso y consiste en que luego de ser identificado el riesgo, se analiza con la finalidad de asignar el nivel que este pudiera tener en caso de que ocurriera. Este nivel puede determinar atreves de su valor cualitativo o cuantitativo y se clasificaran desde muy bajo hasta muy extremos.

4. **Evaluación Y Priorización De Riesgo:** En esta fase se evaluara el nivel de riesgo, con la finalidad de clasificarlo en aceptable o no.

5. **Tratamiento De Riesgo:** En esta fase se tomara la acción que se realizara para tratar el riesgo identificado y priorizado, de acuerdo con sus significancia. Las forma de definas para tratar el riesgo son:

   - **Mitigándolo:** Se establecen los controles necesarios para reducir en su mínima expresión el riesgo.

- **Aceptándolo:** Se acepta el riesgo, se aprende a convivir con el siempre y cuando el nivel de este sea mínimo.
- **Transfiriéndolo:** Se transfiere el riesgo a un tercero, realizado bajo un contrato las pautas o sanciones necesarias que se aplicarían en caso de que el riesgo se materialice y el tercero no responda adecuadamente.
- **Evitándolo:** Se deja de realizar la activada que provoca o puede provocar el riesgo, para así no tener que enfrentarse a él, es la metodología que menor uso tiene.

6. **Revisión Y Monitoreo Continuo:** Es la fase fundamental e integrar del proceso de manejo de riesgo, en donde garantiza la constante actualización de los riesgos que podría enfrentar la organización. Así también se consigue monitorear la efectividad de los riesgos anteriormente identificados y ajustados. Como se ve en la figura este punto es el centro de comunicación de los demás debido a que cada paso debe estar bajo revisión y monitoreo continuo.

3.4 Control De Riesgos

El control de riesgos presenta las medidas o acciones para minimizar o eliminar el impacto de un posible aprovechamiento de una vulnerabilidad. A continuación se presentan los posibles controles aplicables en el Ministerio de Educación de República Dominicana:

Vulnerabilidad. Desperfectos en el cableado, poca protección de sistemas de detección y control de incendios fuera de funcionamiento.

Posible control: Procurar la puesta en funcionamiento del sistema general de control de incendios, verificar el estado del cableado constantemente

Vulnerabilidad: Falta de instalación de sensores de humedad, de químicos e hidrogeno y de polvo.

Posible control: Instalación de sensores de humedad, temperatura, polvo, hidrógeno.

Vulnerabilidad: Falta de tierra eléctrica en la edificación, falta de regulador o protector ante una variación de voltaje.

Posible control: Instalación de tierras y reguladores de voltaje.

Vulnerabilidad: No contar con una política de mantenimiento y actualización de los equipos debidamente formada.

Posible control: Desarrollar los procedimientos adecuados para monitorear constantemente el estado de los equipos, Roadmap para los equipos.

Vulnerabilidad: El no establecimiento de los acuerdos de niveles de servicio debidos, no contar con un debido inventario de sistemas de información.

Posible control: Mantener una comunicación constante con todos los suplidores y asegurarse del diseño correcto de los SLA, supervisar los activos de los equipos incluyendo en estos las licencias.

Vulnerabilidad: Falta de pararrayos, falta de tierra eléctrica en la edificación y falta de regulador o protección ante una variación de voltaje.

Posible control: Instalar pararrayos, instalar tierra eléctrica, protección contra variación de voltaje.

Vulnerabilidad: Inyección de código SQL, falla en los controles de acceso, desactualización de los antivirus, falta de monitoreo de las plataformas de telecomunicación.

Posible control: Establecimiento de un Sistema de Gestión de Seguridad Informática que abarque todas las plataformas y los controles.

Vulnerabilidad: Falta de instalación de sensores de rotura de vidrios, movimiento y vibración, falta de instalación de un sistema de cámaras.

Posible control: Reforzar los controles de seguridad, instalar sensores de rotura de vidrio, movimiento y vibración, cerciorarse de la instalación y correcto funcionamiento de un sistema de cámaras

Vulnerabilidad: No contar con una política de mantenimiento y actualización de los equipos debidamente formada.

Posible control: Desarrollar los procedimientos adecuados para monitorear constantemente el estado de los equipos, Roadmap para los equipos.

Vulnerabilidad: Una ventana abierta o sin protección.

Posible control: Reforzar la estructura para que esta sea más resistente a los vientos e inundaciones, instalación de sensores de rotura de cristales.

Vulnerabilidad: Falta de pararrayos, falta de tierra eléctrica en la edificación y falta de regulador o protección ante una variación de voltaje.

Posible control: Instalar pararrayos, instalar tierra eléctrica, protección contra variación de voltaje.

Vulnerabilidad: El diseño y época de construcción, instalación de sistemas anti sísmicos para los equipos.

Posible control: Reforzar la construcción de la estructura para acondicionarla a los nuevos tiempos y ante movimientos telúricos.

3.5 Identificación y Valoración De Activos

Es necesario identificar los activos de valor de la institución. Para este plan de recuperación de desastre se identificaran los activos de manera resumida que tiene alcance el análisis de riesgos.

Hardware

Cant.	Nombre	Marca	Ubicación
120	Servidores de dominio, aplicaciones, hospedaje, comunicaciones, mensajería y seguridad.	Dell PowerEdge R710 Rack Server	Cede Central
10	Servidores de almacenamiento y respaldo en discos	Dell DX Object Storage Platform	Cede Central
15	Servidor de respaldo en cinta	Dell PowerVault DL Backup	Cede Central
1000	Computadores de escritorio	HP, Dell	Cede Central
	Rack de cableado UTP y fibra óptica		Cede Central

Hardware

Cant.	Nombre	Marca	Ubicación
20	Switch alámbricos	Cisco	Cede Central
3	Routers	Cisco	Cede Central
5	Rack Enclosure de servidores y Switch	Dell PowerEdge 4220 Rack Enclosure	Cede Central
10	KVM Switch Inalámbrico	Dell KVM 2162DS Remote Console Switch	Cede Central
1	Sistema de detección de Incendio	TRIPP Lite	Cede Central
1	Sistema de refrigeración y control de humedad	TRIPP Lite	Cede Central
1	Sistema de UPS	TRIPP Lite	Cede Central

Software

Cant.	Nombre	Marca	Ubicación
1	Sistema de Gestión de Centros Educativos	In house	Cede Central
1	Sistema de Evaluación de Desempeño	In house	Cede Central
1	Sistema de Acompañamiento y Supervisión Educativa	In house	Cede Central
1	Sistema de Gestión de Pruebas Nacionales	In house	Cede Central
1	Sistema de Gestión de Recursos Humanos	In house	Cede Central
1	Sistema de Monitoreo de Red	/	Cede Central
1	Sistema de Monitoreo de Datacenter	DELL	Cede Central
1	Sistemas Proxy de Seguridad	Microsoft	Cede Central
1	SharePoint 2010	Microsoft	Cede Central
1	Outlook Exchange	Microsoft	Cede Central
1	Mensajería y comunicación Lync	Microsoft	Cede Central
1	Office 2010	Microsoft	Cede Central
20	Internet Information Services	Microsoft	Cede Central

Base de datos

Cant.	Nombre	Marca	Ubicación
3	SQL Server Enterprise Edition 2008 R2	Microsoft	Cede Central

Valorización de Activos Críticos (La suma de las tres columnas) Leyenda: 0-2 Muy Baja, 3-5 Baja, 6-9 Media, 10-12 Alta, 13-15 Muy Alta A=Confidencialidad, B=Integridad, C=Disponibilidad				
Activo	**A**	**B**	**C**	**Valorización**
Servidores de dominio, aplicaciones, hospedaje, comunicaciones, mensajería y seguridad.	5	5	5	Muy Alta
Servidores de almacenamiento y respaldo en disco y cinta	5	4	5	Muy Alta
Rack de cableado UTP y fibra óptica	2	3	4	Media
Switches alámbricos	2	3	3	Media
Routers	5	4	5	Muy Alta
KVM Switch Inalámbrico	4	4	5	Muy Alta
Sistemas de Información Internos	5	5	5	Muy Alta
Aplicaciones de terceros	3	4	4	Alta
Sistemas operativos	3	4	4	Alta
Sistemas de Seguridad	5	5	5	Muy Alta
Motores de base de datos	4	5	5	Muy Alta

3.6 Resumen Ejecutivo del Capítulo

En el capítulo tres se definió la evaluación de riesgo en el que se concluyó que este simplemente calcula las vulnerabilidades y el impacto que se relacionan con los activos de la institución. Luego, se procedió a identificar los riesgos latentes para el MINERD, no sin antes definir riesgo latente, que no es más que la evaluación de las situaciones o circunstancias que podrían significar un posible peligro para la institución si se llegase a materializarse.

Se procedió con la identificación de las amenazas y vulnerabilidades para el MINERD que son las siguientes:

- Huracanes
    - Vulnerabilidad Asociada: Una ventana abierta o sin protección.
- Tormentas Tropicales y Eléctricas
    - Vulnerabilidad Asociada: Falta de pararrayos, falta de tierra eléctrica en la edificación y falta de regulador o protección ante una variación de voltaje.
- Incendio
    - Vulnerabilidad Asociada: Desperfectos en el cableado, poca protección de sistemas de detección y control de incendios fuera de funcionamiento.
- Terremoto
    - Vulnerabilidad Asociada: El diseño y época de construcción.
- Tsunami o Maremoto
    - Vulnerabilidad Asociada: La cercanía a la costa.
- Humedad
    - Vulnerabilidad Asociada: Falta de instalación de sensores de humedad, de químicos e hidrogeno y de polvo.
- Variación Eléctrica
    - Vulnerabilidad Asociada: Falta de tierra eléctrica en la edificación, falta de regulador o protector ante una variación de voltaje.

- Degradación del Hardware
    - Vulnerabilidad Asociada: No contar con una política de mantenimiento y actualización de los equipos debidamente formada.
- Incumplimientos Legales
    - Vulnerabilidad Asociada: El no establecimiento de los acuerdos de niveles de servicio debidos, no contar con un debido inventario de sistemas de información.
- Hackeo, virus informáticos, etc.
    - Vulnerabilidad Asociada: Inyección de código SQL, falla en los controles de acceso, desactualización de los antivirus, vencimiento del licenciamiento, falta de monitoreo de las plataformas de telecomunicación.
- Error humano y acceso del personal.
    - Vulnerabilidad Asociada: Falta de instalación de sensores de rotura de vidrios, movimiento y vibración, falta de instalación de un sistema de cámaras.

En ese mismo orden, se identificó la probabilidad de ocurrencias de riesgos que, sin importar la naturaleza de las mismas se ven sujetas a ser valoradas según su probabilidad de ocurrencia. Se definió el significado de probabilidad para mayor comprensión para luego presentar un análisis de la probabilidad de ocurrencia en el que tuvieron lugar los eventos como terremoto, tsunami o maremoto, huracanes y tormentas, incendios, hacking, problema de climatización, error humano y acceso al personal, inundaciones y por último, fallas eléctricas.

El siguiente paso en este capítulo fue priorizar los riesgos, el cual, se agruparon los activos en conceptos genéricos. Estos activos se agruparon globalmente en lo que se denomina Hardware TI, Sistemas de Información, por estructura física y por equipos eléctricos. Todo esto se presento en una matriz de manera detallada.

Una vez presentada la matriz, se describió el proceso de manejo de riesgos en el cual se tomaran las decisiones en un ambiente de indecisión sobre una acción que va a suceder y sobre el impacto que existiría si esta acción ocurriese. Los pasos que se describieron de manera detallada para la administración del manejo de los riesgos son los siguientes:

- Establecimiento De Contexto.
- Identificación De Riesgo.
- Análisis De Riesgo.
- Evaluación Y Priorización De Riesgo.
- Tratamiento De Riesgo.
- Revisión Y Monitoreo Continuo.

Posteriormente, se presentaron los controles de riesgos del MINERD, definiendo primeramente que estos son las medidas o acciones para minimizar o eliminar el impacto de un posible aprovechamiento de una vulnerabilidad. Se presentaron las vulnerabilidades identificadas y sus posibles controles detalladamente. Por último, se identificaron los activos de valor para la institución, de los cuales, se resumió lo que esta investigación tiene alcance.

Capitulo IV

Análisis De Impacto Del Negocio (BIA)

4.1 Análisis De Impacto Del Negocio (BIA)

El objetivo principal, con la realización de esta evaluación de impacto, es pretender establecer e identificar todos los procesos realizados en el Ministerio de Educación República Dominicana (MINERD), para a partir de esto identificar los críticos para las actividades que realiza.

A partir de la identificación de los procesos críticos se procederá a estimar los costos relacionados con estos y los tiempos máximos que cada uno de estos puede estar fuera de servicio. Así también se determinará la cantidad tolerable en pérdida de datos que las áreas pueden soportar.

Para obtener esta información se apoyará en el formulario en el anexo II, el cual será entregado a los directores cada departamento. Esto para que la información sea aportada por los individuos que tienen mayor conocimiento tanto de las funciones como de su impacto.

La información obtenida será base para el diseño de las estrategias de recuperación de cada uno de los procesos críticos identificados.

Alcance: las áreas funcionales que abarcará la evaluación de impacto son:

Servicios Pedagógicos

Estos servicios que corresponden a la función sustantiva del MINERD, se ofrecen permanentemente a nivel nacional y comprende los niveles Inicial, Básico y Media, en los tipos formal, no formal e informal. Estos servicios son

ofrecidos a través de una estructura académica conformada por niveles, ciclos, grados, modalidades y subsistemas.

Servicios de Apoyo Administrativo

Responsables de gestionar, ejecutar y controlar las adquisiciones y suministros de los recursos financieros, materiales y humanos necesarios para apoyar en la consecución de los propósitos y fines de la educación dominicana.

Servicio de Planificación

Área técnica asesora encargada de formular y proponer las políticas y los planes de desarrollo educativo, que fortalezcan los procesos de toma de decisiones para garantizar la eficiencia del Sistema Educativo Nacional.

Servicio de Creación y Mantenimiento de Infraestructura Física Escolar

Área responsable de la previsión y determinación de necesidades de infraestructuras físicas, de establecer la normativa para su ubicación y diseño, y de coordinar y supervisar las construcciones a nivel nacional.

Servicio de Tecnología y Sistema de Información

Responsable de coordinar, ejecutar y dar seguimiento al análisis, diseño y programación de los sistemas de información, y de dar apoyo en materia de instalación, manejo y mantenimiento de equipos informáticos del Ministerio de Educación.

Servicio de Financiamiento y Cooperación Externa

Esta área trabaja con colaboración técnica y económica proveniente de organismos nacionales e internacionales, para apoyar la acción educativa en el MINERD, y cumplen un período determinado de ejecución.

Servicio de Monitoreo y Evaluación de la Calidad Educativa

Área técnica asesora encargada de velar por la eficiencia y eficacia del Sistema Educativo Nacional, garantizando el control de los estándares de calidad en la educación dominicana mediante acciones permanentes de supervisión, evaluación y seguimiento.

4.2 Definición De Niveles De Impacto

Los niveles de impacto definidos para este DRP son los siguientes:

Vital. Este nivel de impacto indica que el proceso es indispensable y de gran valor para la organización. Para los procesos clasificados en este nivel se debe prestar especial atención al momento del desarrollo de estrategias dado que no se pueden excluir del DRP. Este nivel de impacto indica que tiempo máximo que estos pueden estar inhabilitados o fuera de servicio es menor a 4 horas.

Crítico. Este nivel de impacto que de suma importancia pero la organización no depende estos para realizar sus funciones principales. Este nivel de impacto indica que tiempo máximo que estos pueden estar inhabilitados o fuera de servicio está comprendido entre 4 y 8 horas.

Esencial. Este nivel de impacto indica que el proceso brinda información a sistemas de mayor nivel de importancia. Este nivel de impacto indica que

tiempo máximo que estos pueden estar inhabilitados o fuera de servicio está comprendido entre 8 y 24 horas.

Importante. Este nivel impacto indica que el proceso es de jerarquía inferior y que el proceso solo maneja información para sistemas o subprocesos de menor nivel y que por ende no afectan otros procesos indispensables. Este nivel de impacto indica que tiempo máximo que estos pueden estar inhabilitados o fuera de servicio está comprendido entre 1 y 3 días.

No critico. Este nivel de impacto indica que es un proceso no indispensable para las actividades de la organización y que se puede prescindir de este por mucho tiempo en caso de un desastre o evento no programado. Este nivel de impacto indica que tiempo máximo que estos pueden estar inhabilitados o fuera de servicio está comprendido entre 5 y 5 días.

4.3 Identificación De Procesos Y Método De Ejecución

A continuación se muestra un cuadro que identifica los procesos y sus métodos de ejecución. La leyenda de sistema es como sigue:

- SAS (Sistema de Acompañamiento y Supervisión Educativa)
- SPN (Sistema de Consulta de Pruebas Nacionales)
- SGCE (Sistema de Gestión de Centros Educativos)
- SARH (Sistema de Administración de Recursos Humanos)
- SED (Sistema de Evaluación al Docente)

Cuadro de Procesos por Áreas y Ejecución			
Departamento Área	**Procesos**	**Tipo Procesos**	**Sistemas**
Servicios Pedagógicos	Programas de pedagogía escolar para los diferentes niveles	Manual	
	Selección de materiales educativos	Manual	
	Análisis de calidad pedagógica	Automatizado	SAS
	Gestión de Resultados pruebas nacionales	Automatizado	SPN
Servicio de Planificación	Nivel de cumplimiento del calendario y horario escolar	Automatizado	SGCE
	Datos generales de centros educativos que han ingresado al sistema	Automatizado	SGCE
	Estudiantes matriculados por servicio, centro, grado y sección con docente encargado	Automatizado	SGCE
	Matrículas por sección y asignación de docentes	Automatizado	SGCE
	Asignación docente por asignatura	Automatizado	SGCE
	Suspensiones y sus causas	Automatizado	SGCE
	Relación de estudiantes inscritos – Todos los grados	Automatizado	SGCE
Servicio de Creación y Mantenimiento de Infraestructura Física Escolar	Estructuras, servicios y espacios de plantas físicas	Automatizado	SGCE
	Gestión de centros educativos, administración	Automatizado	SGCE
Servicio de Monitoreo y Evaluación de la Calidad Educativa	Análisis de indicadores educativos de toda la región	Automatizado	Análisis de Indicadores
	Análisis de calidad de la educación	Automatizado	SAS
	Gestión de centros educativos, administración	Automatizado	Análisis de Indicadores

Cuadro de Procesos por Áreas y Ejecución			
Departamento Área	**Procesos**	**Tipo Procesos**	**Sistemas**
Servicios de Apoyo Administrativo	Gestión de recursos humanos	Automatizado	SARH
	Gestión administrativa y financiera	Automatizado	SARH
	Administración de personal	Automatizado	SARH
	Evaluación al docente		SED
	Capacitaciones y entrenamientos	Manual	
Servicio de Tecnología y Sistema de Información	Gestión de usuarios	Automatizado	Windows
	Creación y administración de sistemas	Automatizado	Office, emails, SharePoint
	Soporte a usuarios	Automatizado	Lync, emails, SharePoint
	Gestión y administración de comunicaciones	Automatizado	Lync, emails, SharePoint
	Administración de infraestructura tecnológicas a nivel nacional	Automatizado	Sistema de Monitoreo de Infraest.
	Gestión de prest. de equipos	Manual	Office
	Gestión de instalación y mantenimiento de equipos	Manual	Office, emails, SharePoint
	Capacitación técnica a usuarios	Automatizado	Office, emails, SharePoint
	Administración y gestión de portales	Automatizado	Joomla
	Planificación de proyectos	Automatizado	Office, emails, SharePoint
Servicio de Financiamiento y Cooperación	Administración de donaciones	Automatizado	Office, emails, SharePoint

Cuadro de Procesos por Áreas y Ejecución			
Departamento Área	**Procesos**	**Tipo Procesos**	**Sistemas**
Externa	Gestión de cooperación internacional	Automatizado	Office, emails, SharePoint
	Gestión de financiamiento	Automatizado	Office, emails, SharePoint

4.4 Identificación De Procesos Críticos Apoyados En TI

A continuación se muestra un cuadro con la identificación de los procesos críticos identificados, apoyados por la Dirección General de Tecnología de Información y Comunicaciones (DGTIC).

Servicios Pedagógicos		
Nombre Del Proceso	**Descripción Del Proceso**	**Sistema Que Lo Soporta**
Matriculación De Pruebas Nacionales	Se encarga del registro del estudiantado que aplica para las pruebas nacionales	SGCE
Relación de estudiantes – Pruebas Nacionales	Se encarga de establecer la relación entre estudiantes, regionales, direcciones y centros externos	SGCE
Análisis de calidad pedagógica	Se encarga de manejar las consideraciones de lugar estableciendo parámetros para medir el nivel de pedagogía	SAS
Gestión de Resultados pruebas nacionales	Se encarga de todo lo relacionado con los resultados de las pruebas desde el registro hasta alimentación hasta la publicación y alimentación de otros sistemas	Sistema de Consulta de Pruebas nacionales

Servicio de Creación y Mantenimiento de Infraestructura Física Escolar		
Nombre Del Proceso	**Descripción Del Proceso**	**Sistema Que Lo Soporta**
Estructuras, servicios y espacios de plantas físicas	Se utiliza para registrar los centros con su descripción y características y los servicios con los cuales este cuenta	SGCE
Gestión de centros educativos, administración	Se utiliza para solicitar la compra, manejo y condición de los activos en los centros	SGCE

Servicio de Planificación		
Nombre Del Proceso	**Descripción Del Proceso**	**Sistema Que Lo Soporta**
Nivel de cumplimiento del calendario y horario escolar.	Se utiliza para la supervisión del cumplimiento de fechas del calendario académico y los horarios en todos los centros a nivel nacional.	SGCE
Datos generales de centros educativos que han ingresado al sistema.	Se utiliza para el registro de los centros como unidad o elemento del sistema con datos como: Ubicación, Cantidad de aulas, etc.	SGCE
Estudiantes matriculados por servicio, centro, grado y sección con docente encargado.	Se utiliza para registrar los estudiantes asociando estos a centros, regionales y direcciones.	SGCE
Matrículas por sección y asignación de docentes.	Se utiliza para registrar los profesores o docentes asociándolo a centros, estudiantes, regionales y direcciones.	SGCE
Asignación docente por asignatura.	Se utiliza para asignación por las asignaturas a docentes.	SGCE
Suspensiones y sus causas.	Se utiliza para el registro de las suspensiones de clases, solicitando la razón o motivo.	SGCE
Relación de estudiantes inscritos – Todos los grados.	Se utiliza para asociar los docentes a los estudiantes por grado y asignatura.	SGCE

Servicio de Monitoreo y Evaluación de la Calidad Educativa		
Nombre Del Proceso	**Descripción Del Proceso**	**Sistema Que Lo Soporta**
Análisis de indicadores educativos de toda la región.	Este procura que los indicadores educativos propuestos en el plan de educación, estén cumpliéndose.	SGCE
Análisis de calidad de la educación.	Se analiza la calidad con que se imparten las clases y como están reaccionando los estudiantes.	SAS
Gestión de centros educativos, administración.	Este proceso verifica los diferentes centros a nivel nacional y procura que la administración se lleve a cabo.	SGCE

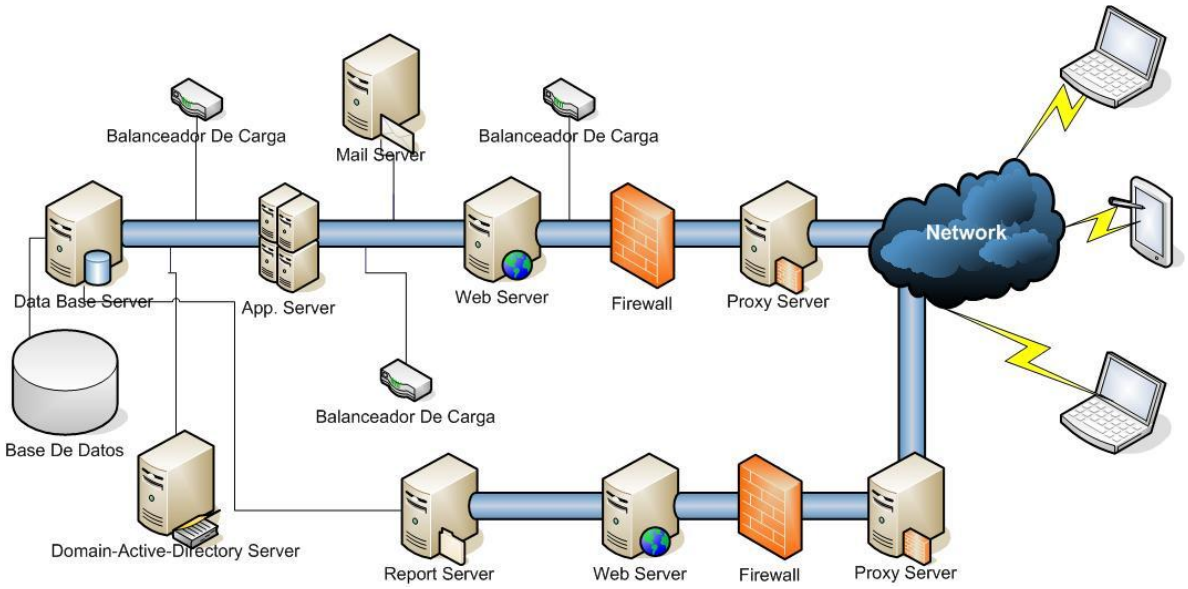
Servicios de Apoyo Administrativo		
Nombre Del Proceso	**Descripción Del Proceso**	**Sistema Que Lo Soporta**
Gestión de recursos humanos.	Gestiona la nómina de todos los empleados y maestros, brinda el servicio y la información que estos necesitan en cuanto a solicitudes, descuento, cooperativa.	SARH
Gestión administrativa y financiera.	Este proceso está en medio entre el gobierno central y el ministerio para la gestión de los recursos financieros.	SARH
Administración de personal.	Se gestiona la contratación y ubicación del personal.	SARH
Evaluación al docente.	Se evalúa a cada maestro para conocer su rendimiento.	SED

Servicio de Tecnología y Sistema de Información		
Nombre Del Proceso	**Descripción Del Proceso**	**Sistema Que Lo Soporta**
Soporte a usuarios.	A nivel nacional se brinda soporte de hardware y software a los docentes, centros educativos y empleados.	Lync, emails, SharePoint
Gestión y administración de comunicaciones.	Este proceso gestiona una comunicación de todos los docentes, estudiantes, centros educativos y empleados a nivel de emails, la herramienta de voz y chat (Lync).	Lync, emails, SharePoint
Administración de infraestructuras tecnológicas a nivel nacional.	Se administran los laboratorios informáticos de los centros educativos públicos y el Datacenter principal en la cede.	Sistema de Monitoreo de Infraestructura.

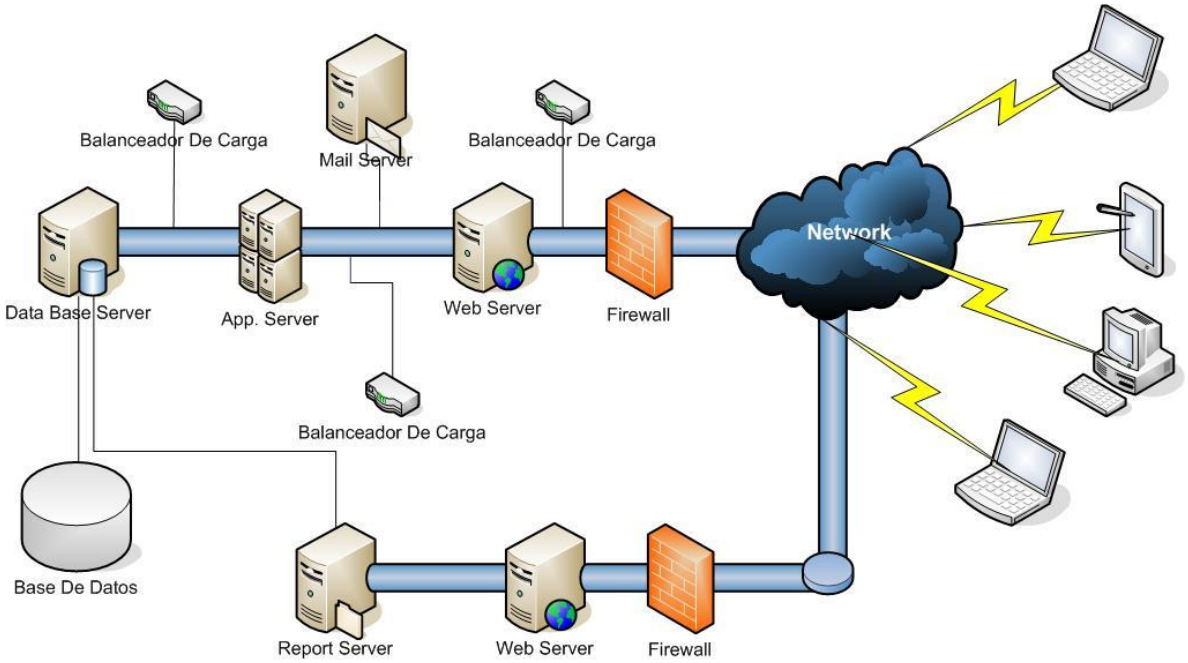
4.5 Flujo Gramas Y Dependencias De Procesos Críticos Apoyados En TI

Todos los procesos críticos apoyados en TI que fueron identificados en el acápite anterior, para su funcionamiento necesitan de una serie de sistemas de información (Hardware y Software), los cuales están comprendidos entre los siguientes esquemas o flujo de dependencias:

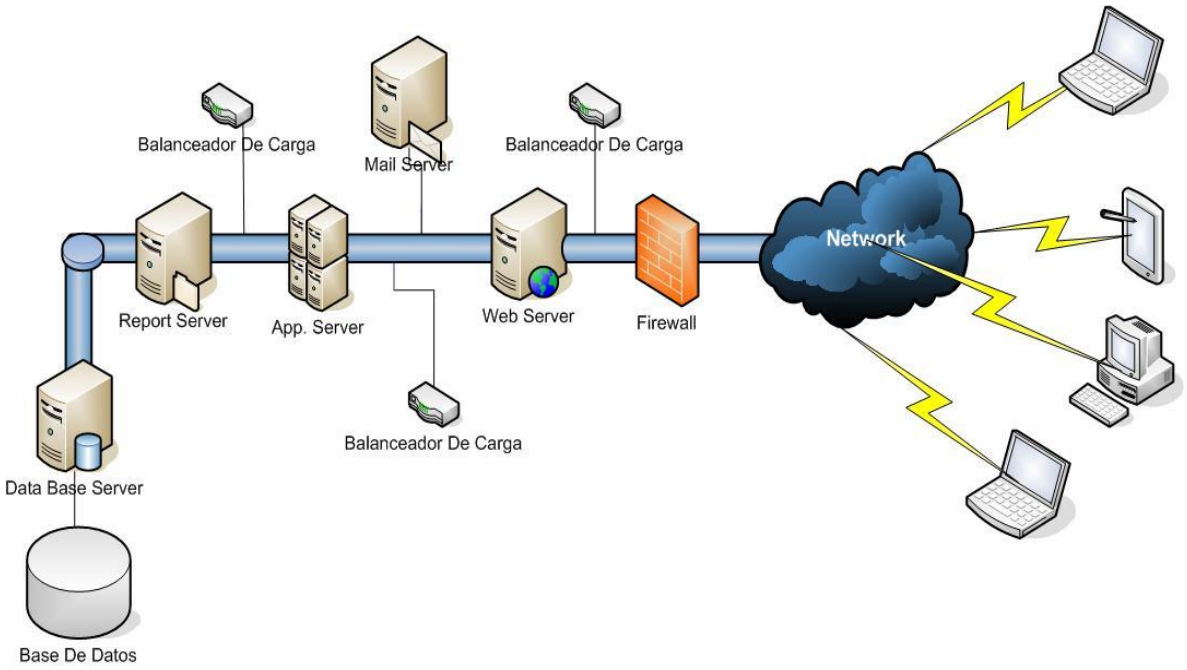
El **Sistema De Gestión De Centro Educativo (S.G.C.E)** para su debido funcionamiento requiere de servidores de base de datos, balanceadores de cargar antes de cada servidor, varios web server, servidores de correo, servidores de reporte, muro de fuegos o firewall, servidores Proxy, redes internas (cableado UTP, Switch, Router) y las líneas de internet que soportan la conexiones, como se muestra en el siguiente esquema:



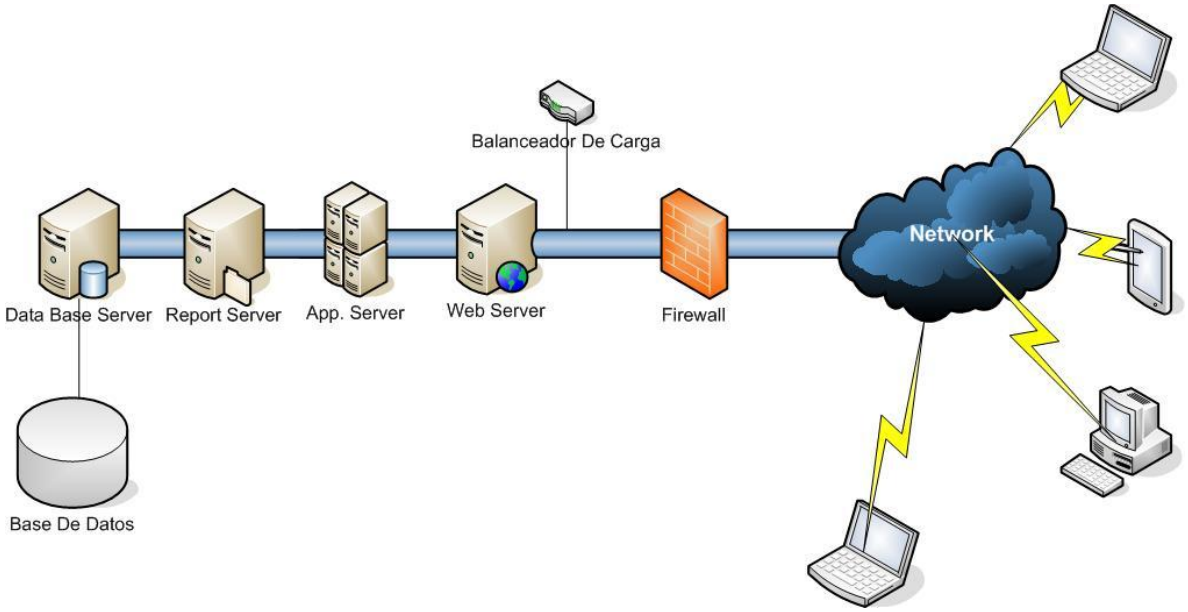
El **Sistema De Evaluación De Desempeño (S.E.D)** para su debido funcionamiento requiere de servidores de base de datos, balanceadores de cargar antes de cada servidor, varios web server, servidores de correo, servidores de reporte, muro de fuegos o firewall, redes internas (cableado UTP, Switch, Router) y las líneas de internet que soportan la conexiones, como se muestra en el siguiente esquema:



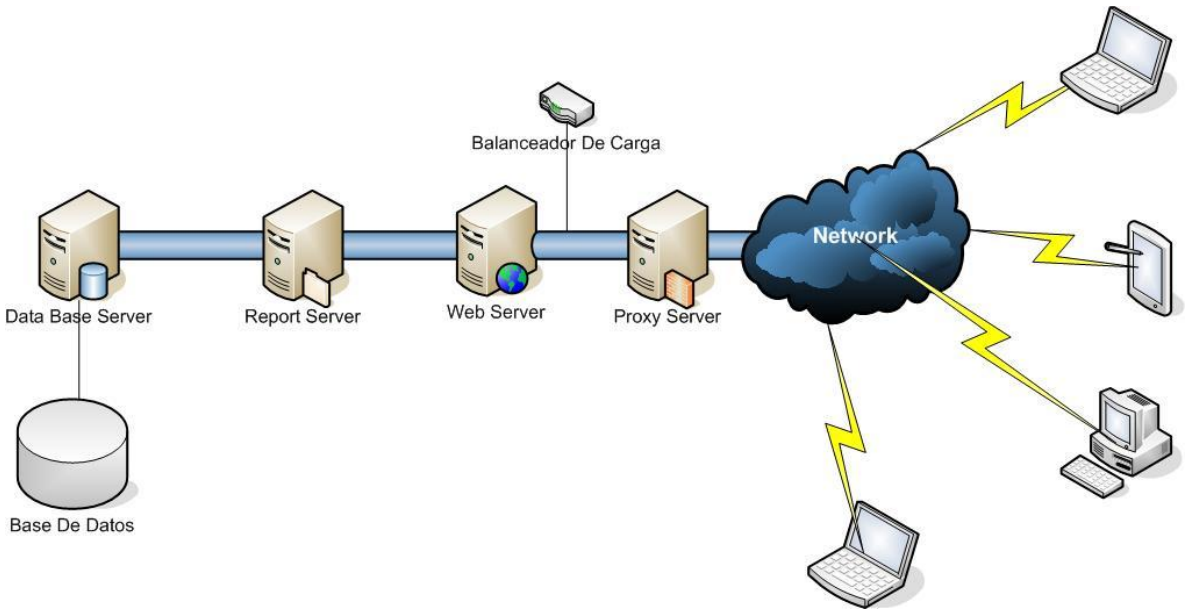
El **Sistema De Acompañamiento Y Supervisión Educativa (S.A.S)** para su debido funcionamiento requiere de servidores de base de datos, balanceadores de cargar antes de cada servidor, servidores de aplicación, varios web server, servidores de correo, servidores de reporte, muro de fuegos o firewall, redes internas (cableado UTP, Switch, Router) y las líneas de internet que soportan la conexiones, como se muestra en el siguiente esquema:



El **Sistema De Análisis De Indicadores (S.A.I)** para su debido funcionamiento requiere de servidores de base de datos, balanceadores de cargar antes de cada servidor, servidores de aplicación, varios web server, servidores de correo, servidores de reporte, muro de fuegos o firewall, redes internas (cableado UTP, Switch, Router) y las líneas de internet que soportan la conexiones, como se muestra en el siguiente esquema:



El **Sistema De Prueba Nacionales (S.P.N)** para su debido funcionamiento requiere de servidores de base de datos, balanceadores de cargar antes de cada servidor, varios web server, servidores de reporte, servidor Proxy, redes internas (cableado UTP, Switch, Router) y las líneas de internet que soportan las conexiones, como se muestra en el siguiente esquema:



4.6 Evaluación De Impacto MTD, RTO, RPO, RTA Y Financiero.

Ministerio de Educación República Dominicana (MINERD) *Matriz del Análisis de Impacto del Negocio Enero-Abril 2012*								
Departamento o área	**Proceso**	**Sistemas de Apoyo**	**MTD (Horas)**	**RPO (Horas)**	**RTO (Horas)**	**RTA (Horas)**	**Impacto Financiero (Días)**	**Nivel De Impacto**
Servicios Pedagógicos	Matriculación De Pruebas Nacionales.	SGCE	4	1	2	2	$ 750,000.00	VITAL
	Relación de estudiantes – Pruebas Nacionales.	SGCE	4	1	1	2	$ 750,000.00	VITAL
	Análisis de calidad pedagógica.	SAS	48	24	32	40	$ 15,000.00	IMPORTANTE
	Gestión de Resultados pruebas nacionales.	SPN	50	0	35	45	$ 7,000.00	IMPORTANTE
Totales Promedio:			**27**	**7**	**18**	**22**	**$ 1,522,000.00**	**VITAL**
Servicio de Planificación	Nivel de cumplimiento del calendario y horario escolar.	SGCE	4	0	2	3	$ 150,000.00	VITAL
	Datos generales de centros educativos que han ingresado al sistema.		8	2	5	6	$ 150,000.00	CRITICO
	Estudiantes matriculados por servicio, centro, grado y sección con docente encargado.		6	1	3	5	$ 200,000.00	ESENCIAL

Ministerio de Educación República Dominicana (MINERD)

Matriz del Análisis de Impacto del Negocio Enero-Abril 2012

Departamento o área	Proceso	Sistemas de Apoyo	MTD (Horas)	RPO (Horas)	RTO (Horas)	RTA (Horas)	Impacto Financiero (Días)	Nivel De Impacto
Servicio de Planificación	Matrículas por sección y asignación de docentes.		2	0	1	1	$ 200,000.00	VITAL
	Asignación docente por asignatura.		3	0	2	2	$ 250,000.00	VILTAL
	Suspensiones y sus causas.		24	5	12	14	$ 15,000.00	IMPORTANTE
	Relación de estudiantes inscritos – Todos los grados.		4	0	2	3	$ 250,000.00	VILTAL
Totales Promedio:			**7**	**1**	**4**	**5**	**$ 1,215,000.00**	**VITAL**
Servicio de Creación y Mantenimiento de Infraestructura Física Escolar.	Estructuras, servicios y espacios de plantas físicas.	SGCE	25	10	18	20	$ 00,000.00	IMPORTANTE
	Gestión de centros educativos, administración.		26	10	18	20	$ 110,000.00	IMPORTANTE
Totales Promedio:			26	10	18	20	$ 210,000.00	IMPORTANTE
Servicio de Monitoreo y Evaluación de la Calidad Educativa	Análisis de indicadores educativos de toda la región.	SGCE	24	12	16	20	$ 5,000.00	IMPORTANTE
	Análisis de calidad de la educación.	SAS	48	20	30	35	$ 15,000.00	IMPORTANTE

Ministerio de Educación República Dominicana (MINERD)

Matriz del Análisis de Impacto del Negocio Enero-Abril 2012

Departamento o área	Proceso	Sistemas de Apoyo	MTD (Horas)	RPO (Horas)	RTO (Horas)	RTA (Horas)	Impacto Financiero (Días)	Nivel De Impacto
	Gestión de centros educativos, administración.	SGCE	24	12	18	22	$ 4,500.00	ESENCIAL
Totales Promedio:			32	15	21	26	$ 24,500.00	IMPORTANTE
Servicios de Apoyo Administrativo	Gestión de recursos humanos.	SARH	4	0	2	2	$ 125,000.00	VITAL
	Gestión administrativa y financiera.	SARH	2	0	1	2	$ 115,000.00	VITAL
	Administración de personal.	SARH	12	2	8	10	$ 60,000.00	ESENCIAL
	Evaluación al docente.	SED	24	2	12	14	$ 35,000.00	ESENCIAL
Totales Promedio:			11	1	6	7	$ 335,000.00	VITAL
Servicio de Tecnología y Sistema de Información.	Soporte a usuarios.	Lync, emails, SharePoint.	72	10	24	48	$ 40,000.00	IMPORTANTE
	Gestión y administración de comunicaciones.	Lync, emails, SharePoint.	2	0	1	1	$ 2,000,000.00	VITAL
	Administración de infraestructura tecnológica a nivel nacional.	Sistema de Monitoreo de Infraestructura.	2	0	1	1	$ 11,000,000.00	VITAL
Totales Promedio:			25	3	9	17	$ 13,040,000.00	VITAL

4.7 Resumen Ejecutivo Del Capítulo

Se estableció y se identificó todos los procesos del MINERD para así separar los procesos críticos. Luego, se procedió a estimar los costos relacionados con estos, los tiempos máximos en que puedan estar fuera de servicio y se determinó la cantidad tolerable en pérdida de datos que las áreas pueden soportar.

El alcance se determinó por las siguientes áreas:

- Servicios Pedagógicos
- Servicios de Apoyo Administrativo
- Servicio de Planificación
- Servicio de Creación y Mant. de Infraestructura Física Escolar
- Servicio de Tecnología y Sistema de Información
- Servicio de Financiamiento y Cooperación Externa
- Servicio de Monitoreo y Evaluación de la Calidad Educativa

En ese mismo sentido se tomó en cuenta los niveles de impacto que son los siguientes:

- **Vital.** Este nivel de impacto indica que el proceso es indispensable y de gran valor para la organización.
- **Crítico.** Este nivel de impacto que de suma importancia pero la organización no depende estos para realizar sus funciones principales.
- **Esencial.** Este nivel de impacto indica que el proceso brinda información a sistemas de mayor nivel de importancia.

- **Importante.** Este nivel impacto indica que el proceso es de jerarquía inferior y que el proceso solo maneja información para sistemas o subprocesos de menor nivel y que por ende no afectan otros procesos indispensables.
- **No crítico.** Este nivel de impacto indica que es un proceso no indispensable para las actividades de la organización y que se puede prescindir de este por mucho tiempo en caso de un desastre o evento no programado.

Se definió los sistemas que soportan los procesos críticos que son:

- SAS (Sistema de Acompañamiento y Supervisión Educativa)
- SPN (Sistema de Consulta de Pruebas Nacionales)
- SGCE (Sistema de Gestión de Centros Educativos)
- SARH (Sistema de Administración de Recursos Humanos)
- SED (Sistema de Evaluación al Docente)

La selección de los procesos críticos se realizó en base a los sistemas mencionados anteriormente, separándolos de los procesos generales identificados por áreas. Además, para cada sistema se realizó un flujo grama que identifica hardware y software que muestra su funcionamiento.

Por último, se creó una matriz de análisis de impacto del negocio del MINERD que visualiza las áreas con sus procesos, los sistemas que lo apoyan y los diferentes acápites que permiten identificar el nivel de impacto.

Capítulo V
Estrategias De Recuperación

5.1 Estrategia De Recuperación

Las estrategias de recuperación se encargan de la evaluación y diseño de las iniciativas más viables para recuperar los sistemas de información de mayor importancia que soportan los procesos críticos antes identificados por el personal seleccionado del MINERD. Esto fue realizado con el apoyo de la DGTIC en la evaluación de impacto.

Las estrategias deberán además de apegarse a las necesidades y prioridades del MINERD, en cuanto a sus procesos críticos, corregir las debilidades identificadas en el análisis de riesgo. Como consecuencia, las estrategias seleccionadas se enfocarán en que los riesgos actualmente identificados sean menores a los que se presentan en el ambiente de producción actual.

Las estrategias de recuperación contemplarán varios puntos o elementos como son:

- Hardware
- Capital o recurso humano
- Localización geográfica
- Software
- Comunicaciones
- Servicio eléctrico

Para los elementos anteriormente se prestará especial atención los costos que impliquen cada uno.

5.2 Estrategia Propuesta

A partir de los datos obtenidos en la evaluación de riesgos y la evaluación de impacto se determinaron las posibles estrategias a presentar a la directiva del MINERD. Para esto se tomó en cuenta que la institución es pública, la importancia para la ejecución y planificación de planes de educación y las leyes locales que regulan el almacenamiento de la información gubernamental indicando que la misma debe de almacenarse en territorio nacional.

Los diagramas presentados a continuación despliegan las estrategias de forma separadas:

1) Estrategia de procesamiento de información mediante computación en la nube (Cloud Computing) y almacenamiento en sitio remoto localmente:

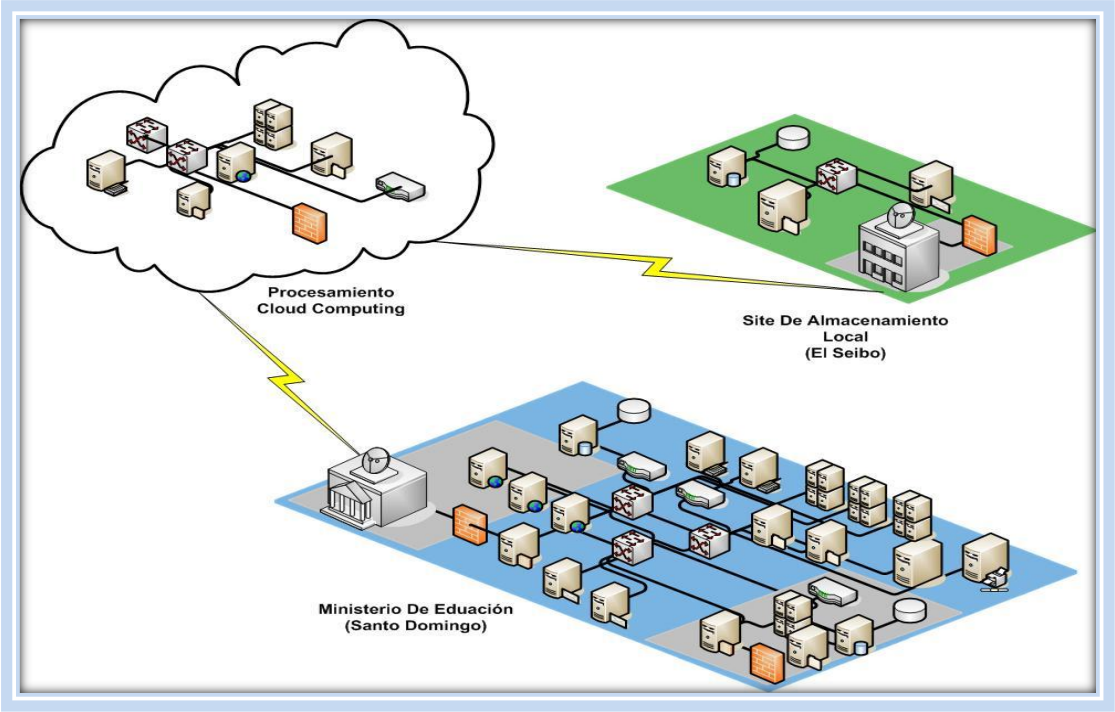


Figura 8

Esta estrategia se basa en la renta o contratación del servicio de computación en la nube pero solo para el procesamiento de datos, posterior a su procesamiento la información será almacenada en un sitio

alterno ubicado en la provincia El Seíbo. Esto porque en los análisis anteriormente realizados se determinó que esta es una provincia con poco riesgo ante catástrofes de grandes magnitudes como son: Inundaciones, terremotos, maremotos, etc.

La estrategia de Cloud Computing solo utiliza una conexión vía Internet lo que disminuye la redundancia en la transmisión o comunicación eliminando costos, pero tiene como desventaja la alta dependencia de acuerdos de servicios (SLA) rigurosos y exigentes por parte de los suplidores.

2) Estrategia de Mirror Site (Sitio espejo) con redundancia en transmisión de datos vía Frame Relay e Internet:

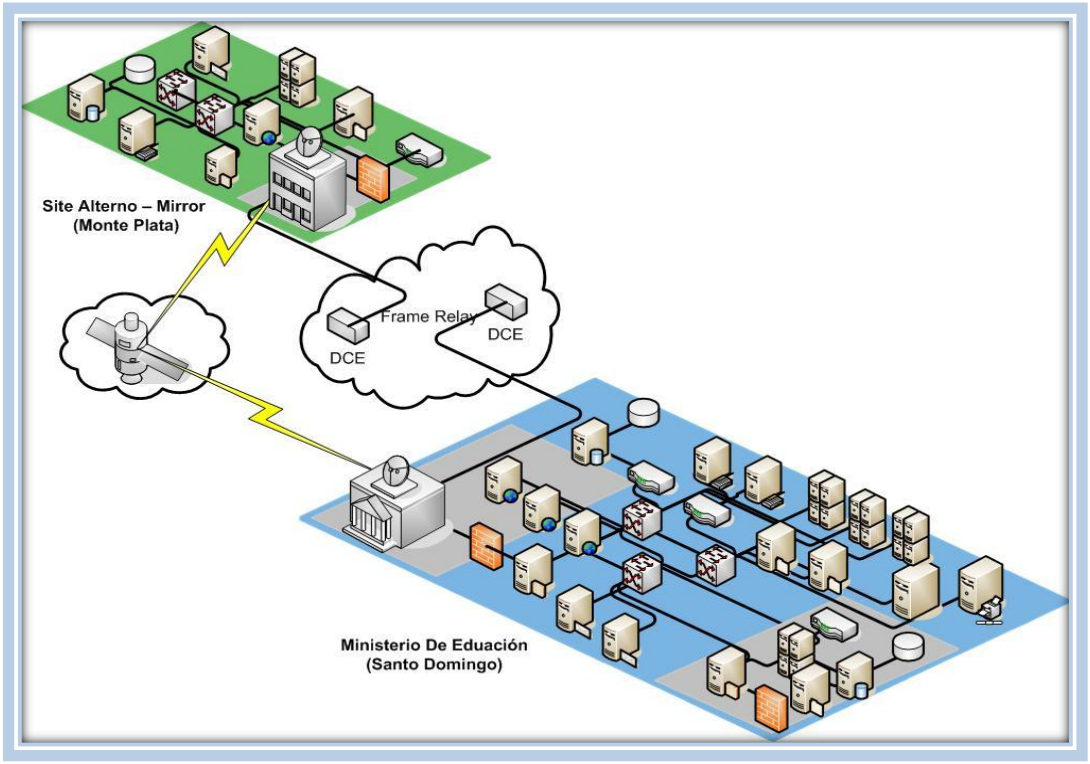


Figura 9

Esta estrategia se basa en la instalación de un sitio alterno ubicado en la provincia de Monte Plata. Dicho sitio poseerá dos enlaces de conexión para asegurar la redundancia, uno utilizando Internet y otro por medio de Frame Relay.

Con esta estrategia se pretende replicar toda la data procesada en la sede principal por medio de la línea Frame Relay con el objetivo de disponer de esta en caso de cualquier desastre o evento no programado.

5.3 Recursos Técnicos y Selección de la Estrategia

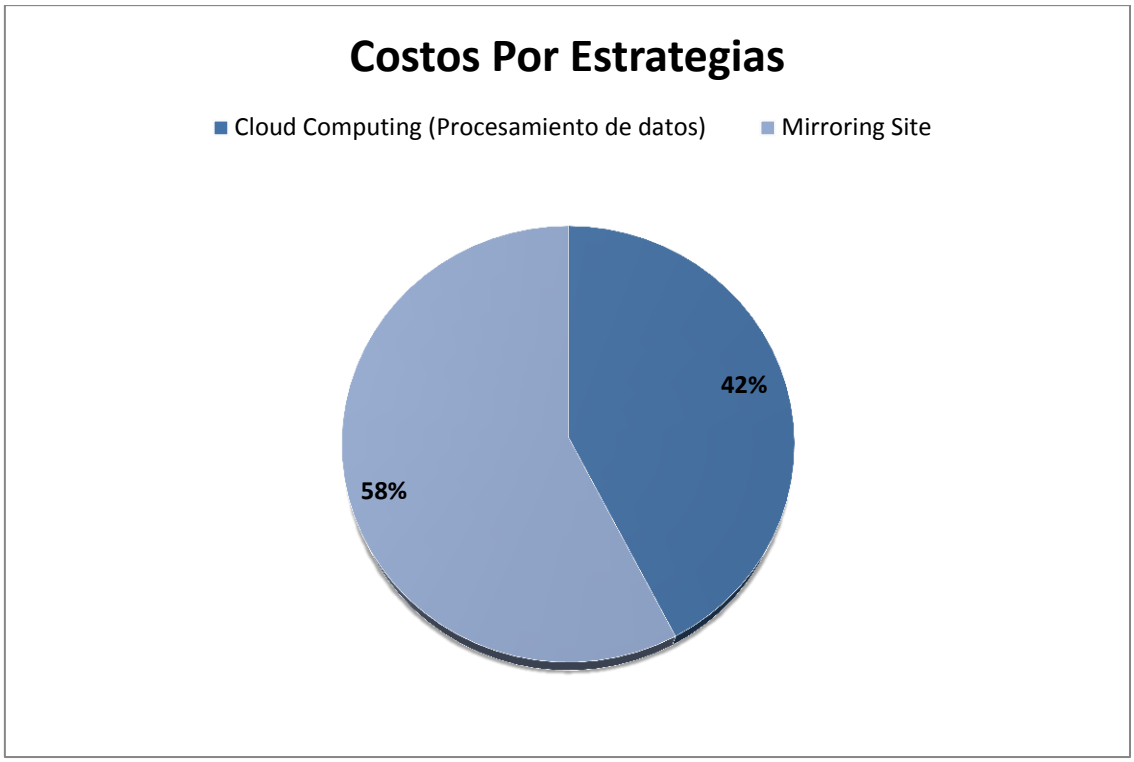
Los recursos técnicos necesarios se refieren a los equipos tecnológicos, equipos no tecnológicos, y el personal necesario que se requiere para que pueda operar la solución alterna que se ha propuesto en el plan de recuperación. Es importante tomar en cuenta varias soluciones para medir la solución más adecuada que se adapte a la necesidad de la organización siempre y cuando cumpla con los requerimientos propuestos en el plan de recuperación de desastres. Además, estos deben seleccionarse para que según el plan, sean el soporte que garantice la continuidad de las operaciones. Esto significa que temporalmente soportaran los sistemas, datos, etc., necesarios que se desean recuperar en caso de un desastre hasta que se recupere la estructura original.

El caso del MINERD se ha seleccionado dos soluciones que pueden adaptarse perfectamente a la necesidad de la que se plantea en capítulos anteriores. Una de estas soluciones es la que se debe implementar y debe seleccionarse de

acuerdo a los criterios de disponibilidad, accesibilidad y costo. A continuación se muestra un cuadro con los componentes necesarios para soportar la continuidad de las operaciones en caso de cualquier emergencia.

		Cloud Computing (Procesamiento de datos)	Mirroring Site
Cant.	**Componentes**	**Costo US$**	**Costo US$**
12	(8 x 1.6GHz CPU, 14GB RAM, 2,040GB Almacenamiento) 250GB Ancho De Banda Windows Azure	$ 1,211.84	$ -
8	Servidores 2.4 GHZ 8 GB RAM	$ -	$ 23,120.00
2	Servidores Base de datos	$ 6,530.00	$ 6,530.00
1	Arreglo de disco 1TB	$ 4,300.00	$ 4,300.00
2	Switches 24	$ 370.00	$ 370.00
1	Routers	$ 500.00	$ 800.00
2	Servicio de Datos Por Parábolas	$ 85,000.00	$ 45,000.00
1	Frame Relay	$ -	$ 18,000.00
10	Cajas de cables 1000 pies	$ 800.00	$ 1,300.00
1	Fibra Óptica	$ 430.00	$ 430.00
1	Planta de Energía Eléctrica 1200 KW	$ 35,000.00	$ 60,000.00
2	UPS200-1200 KW	$ 25,000.00	$ 40,000.00
1	Sistema de enfriamiento	$ 12,000.00	$ 25,000.00
1	Sistema de detección de incendio	$ 5,500.00	$ 10,500.00
4	Mantenimiento y personal	$ 33,248.08	$ 49,872.12
		$ 209,889.92	**$ 285,222.12**

En cuanto a precios de equipos y mantenimiento de la solución, en la siguiente gráfica se puede apreciar el costo de cada estrategia en dólares. Debido a que los equipos no son fabricados en el país, se adquieren en moneda extranjera a la tasa de cambio actual al momento de la compra. Los precios de equipos excepto el mantenimiento incluye la garantía.



Entre las estrategias propuestas y los recursos necesarios que esta conlleva, se puede observar que la estrategia de Cloud Computing resulta más económica. Sin embargo, la estrategia de Mirroring ofrece más accesibilidad y estabilidad en precio. Esto porque Cloud Computing puede variar sus costos en el transcurso del tiempo. Por lo tanto, la estrategia seleccionada para el MINERD es la Mirroring y se indican más razones para ello:

- Más control de la información a nivel lógica y física (Software y Hardware).
- Escalabilidad controlada sin aumentar el precio desproporcionadamente.
- Mejor planificación a largo plazo.

Capítulo VI

Desarrollo Del Plan De Recuperación Ante Desastres

6.1 Objetivo

El objetivo del plan de recuperación ante desastres para el DGTIC es implementar la estrategia seleccionada por la directiva del MINERD. El desarrollo del plan persigue la restauración en el menor tiempo posible de los servicios de la DGTIC que soportan los procesos críticos del MINERD.

Para la elaboración del plan se deben de tomar en cuenta los siguientes elementos:

- Disponibilidad de personal
- Estructuración de equipos
- Disponibilidad de recursos económicos
- Establecimiento o asignación de responsabilidades
- Definición de procedimientos o acciones ante desastres o eventos no programados
- Definición de procedimientos o acciones para la vuelta a normalidad los sistemas del MINERD

6.2 Conformación Y Alcance De Equipos

La conformación de equipo consiste en unificar un grupo de personas las cuales tendrán la responsabilidad de tomar las acciones y decisiones importantes sobre ciertas tareas o actividades específicas antes, durante y después de la ocurrencia de un evento no programado, crisis o catástrofe.

6.2.1 Equipo De Manejo De Crisis

El equipo de manejo de crisis es el que tiene como objetivo principal minimizar los riegos y mantener en armonía el ambiente en caso de ocurrir una situación. Este equipo tiene el compromiso de tomar las decisiones importantes ante la ocurrencia de sucesos o evento. El equipo estará conformado por los siguientes miembros:

Miembros Del Equipo De Manejo De Crisis	**Posición :**	**Director General De DGTIC**
	Departamento o Área :	DGTIC
	Numero De Flota :	849-853-2312
	Grupo De Email :	eq.crisis@see.edu.do
	Posición :	Director De Recurso Humano
	Departamento o Área :	RRHH
	Numero De Flota :	849-853-2311
	Grupo De Email :	eq.crisis@see.edu.do
	Posición :	Director De Seguridad Y Planta Física
	Departamento o Área :	Seguridad
	Numero De Flota :	849-853-2310
	Grupo De Email :	eq.crisis@see.edu.do
	Posición :	Ministra(o) De Educación
	Departamento o Área :	Administración
	Numero De Flota :	849-853-2309
	Grupo De Email :	eq.crisis@see.edu.do

6.2.2 Equipo De Recuperación

El equipo de recuperación es el que tiene el compromiso de llevar a cabo todas las tareas necesarias para ejecutar la estrategia definida con la finalidad de restablecer los servicios en el menor tiempo posible. Así como también realizar las pruebas de lugar necesarias para comprobar que el restablecimiento ha sido éxitos. Este equipo está conformado por los siguientes miembros:

Miembros Del Equipo De Recuperación	**Posición :**	**Administrador De Telecomunicaciones**
	Departamento o Área :	DGTIC
	Numero De Flota :	849-853-2210
	Grupo De Email :	eq.crecuperacion@see.edu.do
	Posición :	Coordinador De Soporte Técnico
	Departamento o Área :	DGTIC
	Numero De Flota :	849-853-2211
	Grupo De Email :	eq.crecuperacion@see.edu.do
	Posición :	Administrador De Base De Datos
	Departamento o Área :	DGTIC
	Numero De Flota :	849-853-2212
	Grupo De Email :	eq.crecuperacion@see.edu.do
	Posición :	Coordinador De Desarrollo De Software
	Departamento o Área :	DGTIC
	Numero De Flota :	849-853-2213
	Grupo De Email :	eq.crecuperacion@see.edu.do
	Posición :	Coordinador De Data Center
	Departamento o Área :	DGTIC
	Numero De Flota :	849-853-2214
	Grupo De Email :	eq.crecuperacion@see.edu.do

6.2.3 Equipo De Logística

El equipo de logística es quién tiene el compromiso de organizar y realizar todas las acciones lógicas relacionadas con la recuperación. Estas alcanzan desde el transporte hasta la alimentación de todo el personal necesario para la ejecución del plan de recuperación. Este equipo está conformado por los siguientes miembros:

Miembros Del Equipo De Logística	**Posición :**	**Director de Planificación De Proyectos Tecnológicos**
	Departamento o Área :	DGTIC
	Numero De Flota :	849-853-2112
	Grupo De Email :	eq.logistica@see.edu.do
	Posición :	Coordinador De Servicio Administrativo
	Departamento o Área :	Administración
	Numero De Flota :	849-853-2111
	Grupo De Email :	eq.logistica@see.edu.do
	Posición :	Contralor General
	Departamento o Área :	Administración
	Numero De Flota :	849-853-2110
	Grupo De Email :	eq.logistica@see.edu.do
	Posición :	Coordinador De Transporte
	Departamento o Área :	Administración
	Numero De Flota :	849-853-2109
	Grupo De Email :	eq.logistica@see.edu.do

6.2.4 Equipo De Relaciones Públicas Y Comunicaciones

Este equipo es el que tiene la responsabilidad de mantener lo más transparente posible la imagen de institución durante y después de la ocurrencia de un evento no programado. Este equipo está conformado por los siguientes miembros:

Miembros Del Equipo De Relaciones Publicas Y Comunicaciones	**Posición :**	**Ministro(a) De Educación**
	Departamento o Área :	Administración
	Numero De Flota :	849-853-1919
	Grupo De Email :	eq.relacionespublic@see.edu.do
	Posición :	Coord. De Relaciones Publicas
	Departamento o Área :	Publicidad
	Numero De Flota :	849-853-1919
	Grupo De Email :	eq.relacionespublic@see.edu.do
	Posición :	Director General DGTIC
	Departamento o Área :	DGTIC
	Numero De Flota :	849-853-1919
	Grupo De Email :	eq.relacionespublic@see.edu.do
	Posición :	Contralor General
	Departamento o Área :	Administración
	Numero De Flota :	849-853-1919
	Grupo De Email :	eq.relacionespublic@see.edu.do

6.2.5 Matriz De Responsabilidades (RACI)

Luego de reuniones con los equipos designados se procedió al establecimiento de tareas y sus responsables utilizando la Matriz RACI. Su función se describió anteriormente en el capítulo 2.

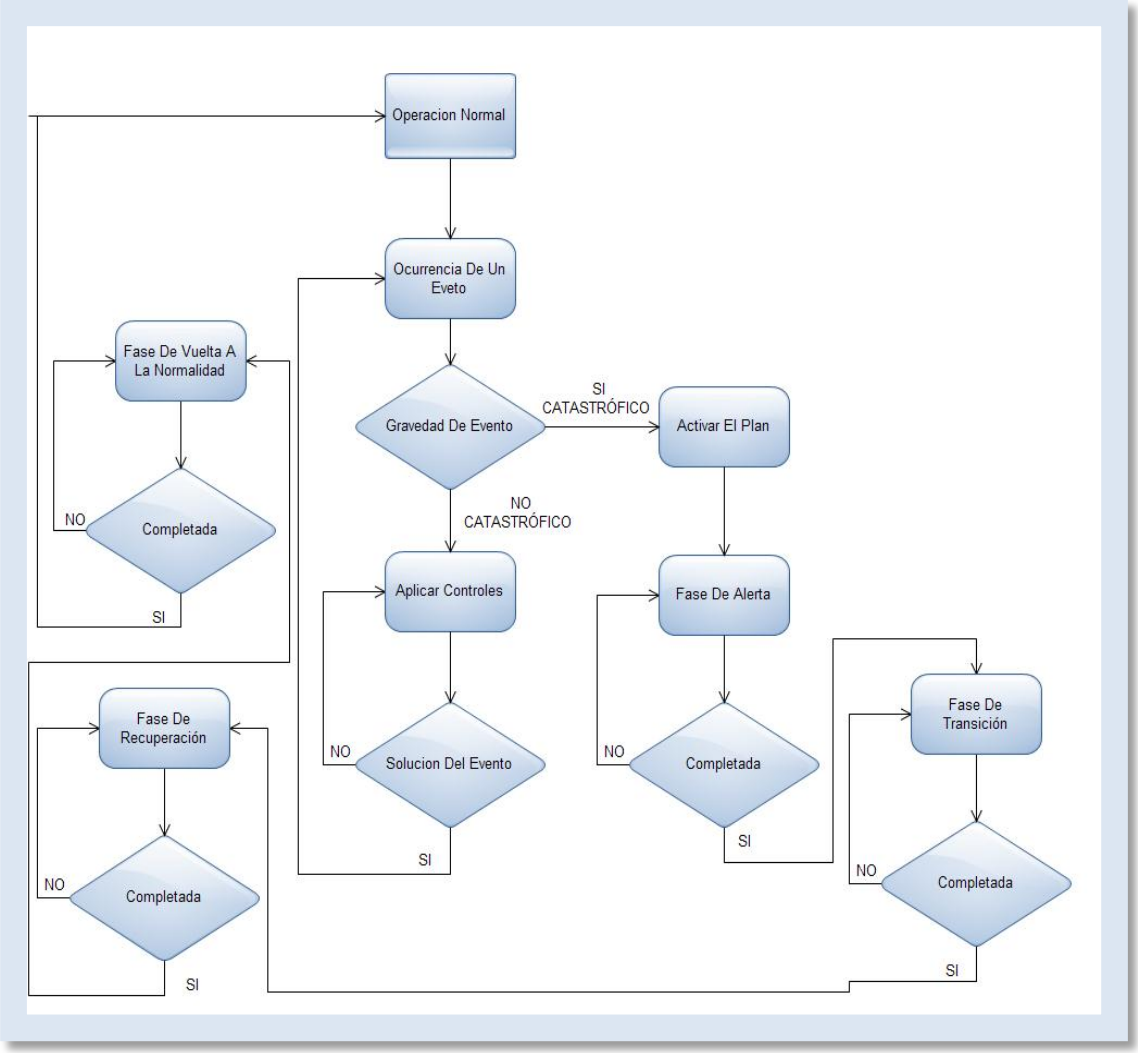
Matriz RACI															
	Equipo de Manejo de Crisis				**Equipo de Recuperación**				**Equipo de Logística**				**Equipos de Relaciones Públicas y Comunicaciones**		
Roles / Actividades	**Análisis de situación**	**Activación del Plan**	**Notificación a equipo de logística**	**Seguimiento al proceso de recuperación**	**Análisis técnico de situación**	**Establecimiento de orden de procesos a recuperar**	**Ejecución de estrategia**	**Verificación de servicios post-recuperación**	**Establecimiento de comunicación entre equipos**	**Establecimiento de contacto con suplidores**	**Transportación de personal**	**Transportación de suplementos**	**Elaboración de comunicados**	**Atención e instrucción de personal**	**Control y mantenimiento de prudencia**
Levantar fase de alerta o alarma	R	R	R	I	I	I	I	I	R	I	I	I	C	I	R
Activación del Plan	R	R	R	R	A	I	I	I	R	A	I	I	A	A	R
Movilización de equipos	I	I	R	I	R	R	R	R	R	R	R	R	C	I	R
Identificación de consecuencias	A	A	I	A	R	I	I	I	R	I	R	I	I	I	I
Identificación de causas del evento	A	A	I	A	R	I	I	I	R	I	R	I	I	I	R
Verificación de respaldos o Back Ups	C	C	C	A	R	R	A	A	A	C	R	R	A	A	R
Restablecimiento de Operaciones	I	I	A	A	A	R	R	A	A	R	R	R	R	R	R
Pruebas de disponibilidad y acceso	I	I	A	A	R	R	R	R	A	A	I	R	A	R	R
Autorización de acceso o uso	C	C	C	C	R	R	R	R	I	I	I	I	I	R	R
Aprobación Administrativa	R	R	R	R	C	C	C	C	A	I	I	I	C	R	R
Retorno de operaciones a estado normal	C	C	C	C	R	R	R	R	A	C	C	I	I	R	R
Documentación y registro de evento y acciones realizadas	I	I	I	I	R	R	R	R	A	A	A	A	I	I	I

6.3 Etapas De Recuperación Por Evento.

En la etapa de recuperación por evento, se indica cómo será el flujo de las decisiones en caso de que ocurriese algún evento no programado o crisis, dependiendo de la magnitud de este se decidirá en si aplicar algún control básico le cual puede ser desde el reinicio de un componente o equipo hasta el remplazo ó se iniciara la activación del plan procediendo a ejecutar las cuatros fase definidas para el funcionamiento de este:

I. **Fase de Alerta:** Esta fase consiste en iniciar la voz de alerta a todos los miembros del equipo de manejo de crisis.
II. **Fase de Transición:** Esta fase consiste en reunir todos los equipos necesarios para llevar a cabo la recuperación de las operaciones perdidas.
III. **Fase de Recuperación:** Esta fase consiste en la realización de las tareas necesarias para recuperar las operaciones que fueron interrumpidas.
IV. **Fase de Retorno a la Normalidad:** Esta fase consiste en retornar a la normalidad como su nombre lo indica todas las operaciones que fueron afectadas en el evento no programado o crisis, evaluando y documentado también el impacto que el género el evento en la institución.

A continuación se muestra la imagen que indica cómo será el flujo de recuperación ante un evento:



Los **eventos catastróficos** son aquellos que inhabilitan 3 o más componentes, afectando la recuperación de los procesos en un tiempo mayor a 24 horas. Obligando así a la directiva a activar el plan de recuperación.

Los **eventos no catastróficos** son aquellos que inhabilitan 2 o menos componentes, permitiendo el funcionamiento parcial de las operaciones o la recuperación de estos en un tiempo menor a 12 horas. Esto permite al equipo de tecnología aplicar los controles necesarios para resolver la problemática.

Los controles que serán aplicados dependerán de la falla que afecten los compontes que se vieron afectados, estos pueden ser:

1) Daño de un Switch, Router o Línea de comunicación**. Control** verificación de configuraciones y en caso necesario remplazar el equipo averiado ó contactar al suplidor para solicitar su apoyo.

2) Daños en componente de hardware en un servidor como son disco duros ó controladora de disco, tarjeta de red, Power Supply, memoria RAM, entre otros. **Control** remplazo del componente averiado ó en caso de ser necesario contactar al suplidor.

3) Corrupción de dato. **Control** restaurar la data del Backup realizado más recientemente.

4) Desconexión de equipo de forma involuntaria o no. **Control** reconectar el equipo y prevenir la ocurrencia futura de la situación.

5) Fluctuación de voltaje en las instalaciones. **Control** colocar los equipos de regulaciones de voltajes necesario para prevenir las fluctuaciones.

6.3.1 Etapa De Alerta

	Acción o Procedimiento
Fase de Alerta	1) Notificación de evento por parte de área de seguridad física
	2) Se notifica al equipo de manejo de crisis
	3) Se solicita evaluación física general a seguridad física
	4) Se evalúa el incidente
	6) Se notifica al equipo de logística para que ubique a todos los equipos

6.3.2 Etapa De Transición

	Acción o Procedimiento
Fase de Transición	1) El equipo de logística realizará las gestiones de lugar para reunir a todos los equipos en el MINERD en caso de ser posible, de lo contrario tendrá la potestad de elegir uno que entienda conveniente
	2) El equipo de logística se encarga del transporte de equipos, dispositivos, copias de seguridad, materiales de oficinas y todo aquel implemento necesario
	3) Se procede a activar el plan de recuperación

6.3.3 Etapa De Recuperación

	Acción o Procedimiento
Fase de Recuperación	1) El equipo de recuperación realiza evaluación técnica haciendo pruebas de funcionamiento de equipos, líneas y conexión entre dispositivos. Para esto utilizará comandos como: Ping, nebtstat, taskmgr, etc…
	2) El equipo de recuperación evalúa la integridad de la data almacenada en el Sitio alterno. Para esto cargará uno de los sistemas y conjuntamente con los líderes de áreas funcionales confirmarán que todo marche en orden.
	2) El equipo de recuperación evalúa los impactos provocados por el incidente.
	3) El equipo de recuperación evalúa las causas del incidente.
	4) El equipo de recuperación verifica las condiciones del sitio alterno tanto físicas como lógicas.
	5) En caso de ser necesario el equipo contactará a los suplidores de los servicios afectados que sean imprescindibles para restaurar el funcionamiento de los procesos críticos para el MINERD. A continuación se detallan estos: **Compañía** **Contacto Directo** **Servicio** CODETEL **Evelyn Herrera** 809-350-2425 Línea de datos TRICOM **Carlos Pérez** 809-243-2934 Línea de datos DELL **Santos Cisneros** 809-435-2087 Servidores HP **Alexis Santos** 809-560-3234 Servidores Cisco **Freddy Grinch** 809-457-6089 Routers/Switch Discom **Agustin Polanco** 809-383-5747 UPS/Planta.

	6) El equipo de recuperación procede a re direccionar el tráfico de la data hacia el Sitio alterno modificando los Iptables en el Router o enrutador. Para esto utilizará los comandos: *"Iptables -t nat -A PREROUTING -s (IP configuradas en la tabla) -p tcp --dport (IP: Puerto destino) -j DNAT --to-destination (IP destino) o Iptables -t nat -A PREROUTING -s (#segmento de red configurado) -p tcp --dport #puerto -j DNAT --to- destination (IP: Puerto destino)"*.
	7) El equipo de recuperación realiza las pruebas de disponibilidad, rendimiento e integridad de los sistemas de información.
	8) El equipo de recuperación procede a informar al equipo de logística los resultados.
	9) El equipo de logística procede a notificar a los demás equipos del Plan

6.3.4 Etapa De Retorno A La Normalidad

	Acción o Procedimiento
Fase de Vuelta a la Normalidad	1) El equipo de manejo de crisis junto al equipo de recuperación proceden con las evaluaciones de lugar para retornar a la normalidad los sistemas de información.
	2) Se notifica al equipo de logística para que proceda con las gestiones de lugar de compra, renta y movilización de los equipos o dispositivos averiados en caso de ser necesario.
	3) Luego de adquiridos o disponibles los sistemas el equipo de recuperación procede con las configuraciones de lugar.
	4) El equipo de recuperación realiza las pruebas de comunicación con el sitio alterno.
	5) El equipo de recuperación procede a re direccionar el tráfico de la data hacia el Sitio alterno modificando los Iptables en el Router o enrutador. Para esto utilizará los comandos: *"Iptables -t nat -A PREROUTING -s (IP configuradas en la tabla) -p tcp --dport (IP: Puerto destino) -j DNAT --to- destination (IP destino) o Iptables -t nat -A PREROUTING -s (#segmento de red configurado) -p tcp --dport #puerto -j DNAT --to- destination (IP: Puerto destino)"*.
	6) El equipo de recuperación realiza las pruebas de disponibilidad, rendimiento e integridad de los sistemas de información.
	7) El equipo de recuperación procede a informar al equipo de logística los resultados.
	8) El equipo de logística procede a notificar a los demás equipos del Plan.

Capítulo VII

Diseño De Pruebas Y Mantenimiento Del Plan

7.1 Pruebas

Una apropiada estrategia para el plan de recuperación es desarrollada e implementada durante esta fase. “Probar el plan de recuperación asegura que la capacidad de la continuidad del negocio permanezca efectiva. No existe una capacidad demostrada o un DRP práctico hasta que este sea probado”.[6]

7.1.1 Objetivos Del Plan De Pruebas.

Los objetivos del plan de prueba se basan en los resultados que se quiere obtener de ella. Se debe definir los objetivos antes de iniciar una prueba. Por lo tanto, antes de probar el DRP propuesto para el MINERD se definirán los objetivos de la prueba a continuación:

- Familiarización de los participantes, los equipos de recuperación en la prueba con sus roles en el evento del desastre.
- Verificar que las estrategias de recuperación propuestas son viables.
- Adiestrar a los líderes de equipo en los procedimientos de ejecución del plan.
- Demostrar que el rendimiento de los sistemas de Backup, sistemas críticos y de las redes del ambiente de prueba son consistentes con los sistemas de ambiente producción.
- Adaptar y actualizar los planes existentes para abarcar nuevos requerimientos resultantes desde el negocio, sistemas, redes o cambio de personal.

[6] HANSCHE, Susan. BERTI, John. HARE, Chris. (2003). Official, (ISC)² Guide To The CISSP Exam. (pp. 698). Boca Raton, Florida. CRC, Press.

- Probar todos los componentes del plan, incluyendo Hardware, Software, personal, data, telecomunicaciones, procedimientos, documentación, transportación, utilidades, sitios de procesamientos alternos, etc., según aplique con los sistemas y operaciones críticos previamente establecidos.

7.2 Tipos De Pruebas

Antes de que inicie una prueba, es necesario saber qué tipo de prueba se realizará. Además de los objetivos seleccionados, se debe documentar el tiempo de la prueba, el día de la prueba e informarlo a los participantes de la prueba.

Existen en la actualidad 5 tipos principales de pruebas[7]. Estos tipos de tratas de una estrategia de prueba del plan de recuperación de desastres son:

- Structured Walk-Through (Prueba sobre papel):
    - Se reúnen los representantes funcionales para revisar el plan en detalle.
    - La estrategia implica un profundo vistazo a cada uno de los pasos del plan y los procedimientos que se invocan en el plan.
    - Se asegura de que las actividades planeadas actualmente están exactamente descritas en el plan.

[7] HANSCHE, Susan. BERTI, John. HARE, Chris. (2003). Official, (ISC)² Guide To The CISSP Exam. (pp. 699). Boca Raton, Florida. CRC, Press.

- Checklist Test (Prueba de lista de verificación):
  - Distribuye copias a cada una de las áreas funcionales
  - Cada área revisa el plan y marca los puntos que están listados para asegurar que el plan se refiere a todas las actividades y todo lo concernido.
- Simulation (Simulación):
  - Todos, los de operaciones y técnicos se reúnen para practicar la ejecución del BCP basado en un escenario manejado para probar la reacción de todas las funciones.
  - Todos los materiales e información disponible de un desastre real se permiten para ser usados en la simulación.
  - La simulación continua hasta el punto de reubicación alterna y el remplazo de los equipos.
- Parallel test (Prueba paralela):
  - Los sistemas críticos se colocan en un sitio alterno para verificar la correcta operación.
  - Los resultados son comparados con las operaciones reales.
  - Se concentra en las operaciones del BCP.
- Full Interruption test (Prueba de interrupción completa):
  - Esta es una prueba completa del BCP.
  - Las operaciones y procesamientos normales son completamente sacados de línea o apagados y conducidos a un sitio alterno, usando los materiales que están disponibles, equipos disponibles con el equipo de personal de recuperación. Esta prueba no es recomendada para empresas grandes.

De acuerdo a las definiciones presentadas de los tipos de pruebas, el elegido para garantizar la efectividad del plan seleccionado para el MINERD, es la llamada “Prueba Paralela”. Esta consistirá en asegurar que los sistemas críticos puedan operar exactamente en un sitio alterno como si fuese producción. Luego, los resultados son comparados entre ambos sitios. Si existe algún inconveniente se van corrigiendo y se va comparando los objetivos de pruebas propuestas.

7.2.1 Definición De Período De Pruebas

El período de prueba deberá ejecutarse una vez al año y luego de una revisión del plan para fines de mantenimiento. Este período es más recomendable entre los meses de febrero y abril, luego de la entrega del presupuesto y antes del inicio de la temporada de huracanes. A continuación se muestra un cuadro de calendarización y responsables de la prueba:

Responsables	Actividad	Fecha	Duración
Equipo de Recuperación	Definición Inicio de Prueba	1 abril	3 horas
	Delegación de Equipo Prueba		
	Delegación de Equipo de Logística Informática		
	Reunión con Equipos seleccionados.		
Equipo de Logística Informática	Coordinar necesidades para la prueba	10 abril	3 horas
	Notificar al equipo de prueba		
	Reunir las necesidades para día prueba	14 abril	8 horas
Equipo de Pruebas Seleccionado	Activación del Site alterno	14 abril	8 horas
	Inicio de pruebas de estrés Site alterno.	15 abril	
	Comprobación de resultados.		
	Documentación de Pruebas		
	Solución de inconvenientes de pruebas		
	Reporte de pruebas para el equipo de recuperación	16 abril	

7.3 Mantenimiento Del Plan De Continuidad

Mientras la organización y sus procesos de negocios continuamente cambian, también lo debe hacer el plan. Actualizar la documentación de un plan de recuperación que esté acorde con la estrategia y dirección de la organización, es de vital importancia para garantizar una recuperación satisfactoriamente.[8]

El MINERD necesita, mínimo una vez al año, modificar y mantener su plan de recuperación para que este actualizado. Si este plan no se actualiza, entonces es muy probable que el plan no funcione al momento de requerirse una recuperación. Por lo tanto, se presenta un cuadro con las técnicas y calendarización del mantenimiento:

Responsables	Actividad	Fecha	Duración
Equipo de Recuperación	Definición Inicio de actualización y mantenimiento del plan	1 febrero	3 horas
	Delegación de Equipo Mantenimiento del plan		
	Delegación de Equipo de Logística Informática		
	Reunión con Equipos seleccionados.		
Equipo de Logística Informática	Coordinar necesidades y requerimientos para el mantenimiento del plan	10 febrero	3 horas
	Reunir y suplir al equipo de mantenimiento lo que necesitan para ejecutar.	14 febrero	8 horas
Equipo de Mantenimiento	Inicio del mantenimiento, se distribuyen copias del plan actual.	15 febrero	152 horas
	Revisión del plan de recuperación actual.		
	Identificación e investigación de cambios según el plan.		
	Documentación de cambios al plan para su actualización.	10 marzo	64 horas
	Eliminación de copias del plan viejo, se distribuye el nuevo.	20 marzo	16 horas
	Reporte de Cambios.	22 marzo	8 horas

[8] HANSCHE, Susan. BERTI, John. HARE, Chris. (2003). Official, (ISC)² Guide To The CISSP Exam. (pp. 700). Boca Ratón, Florida. CRC, Press.

Capítulo VIII
Programa De Capacitación Y Concientización Del Plan

8.1 Programa De Capacitación Y Concientización

El programa de capacitación y concientización del plan de recuperación ante desastre es tan necesario como el plan mismo, ya que, el conocimiento, la cultura y el compromiso que desarrollen las personas de la institución será parte esencial para garantizar el éxito del plan.

En el Ministerio de Educación de la Republica Dominicana (MINERD) se llevaran a cabo una serie de actividades con la finalidad de fomentar en todos los empleados un compromiso con el DRP, así como también, realizar los planes de capacitación necesarios para todo el personal. Esto consistirá en las siguientes estrategias:

- Colocación de afiches informativos con diversidad de colores e imágenes alusivas al tema tratado.
- Circulación de una revista digital mensual
- Envió de correos semanales informativos con contenido de cómo actuar ante la presencia de eventos no programado o crisis, ya sean estos naturales o no, y estadística de catástrofe de alta ocurrencia por temporadas o periodos.
- Propagación de texto, audio y video de informaciones de prevención ó forma de actuar ante la presencia de una problemática o catástrofe.

A continuación se muestra un cronograma de actividades con el contenido ampliado de la misma:

Cronograma De Actividades				
Actividad	**Responsable**	**Contenido**	**Fecha**	**Duración**
Charlas	Equipo De Comunicación	Manejo Del Personal Ante Crisis	1 al 27 de Abril	2 Horas Cada Sección
		Conocimientos De DRP		
		Objetivo Del DRP		
		Porque es necesario Un DRP		
		Prevenciones Naturales		
		Manejo Ante Catástrofes Naturales		
		Catástrofes Naturales Mas Frecuentes		
Seminario	Miembro De Los Bomberos Dominicanos	Prevención Ante Fuego	28 de Abril al 12 de Mayo	2 Horas Cada Sección
		Tipos De Fuegos		
		Tipos De Extintores De Fuego		
		Como actuar Ante Un incendio		
		Incendio Mas Comunes, Y Materiales Mas Inflamables		
		Prevención Y Manejo De Incendio En Data Center		
Taller	Equipo De Comunicación	Manejo De Comunicaciones Ante Crisis	13 al 25 de Mayo	3 Horas Cada Taller
		Utilización De Redes Sociales (Twitter, Face Book, Etc)		
		Comunicación A Clientes Externo En Caso De Crisis		
		Manejo Del Flujo De Información		
		Como Manejar Los Medios De Publicación Ante Crisis		
		Como Accionar Ante Una Crisis O Problemática		
Reunión	Equipo De Manejo De Crisis	Manejo De Crisis	26 de Mayo al 1 de Junio	30 Minutos De Reunión
		Manejo De Riesgo		
		Comunicación Ante Desastre Con Los Clientes		
Desayuno	RRHH	Como Actuar Ante Huracanes, Terremoto.	1 al 25	30 Minutos

Empresarial		Importancia De Tener Un DRP	de Junio	Cada Desayuno
		Importancia De Notar Y Reportar Eventualidades		
		Objetivos De Las Capacitaciones		
Afiches Informativos	RRHH	Estadística De Ocurrencia De Huracanes	Todo El Año	-
		Organigrama De Manejo De Crisis		
		Flujo Ante Un Evento		
		Importancia De Seguir Los Planes		
Revista Digital Mensual	Equipo De Comunicación	Información De Manejo De Crisis	Todo El Año	Mensual
		Importancia De Un DRP		
		Como Actuar Ante Un Evento		
		Importancia De Tener Un Equipo Por Piso		
		Que Acciones Tomar Ante Una Crisis		
Envió De Email Semanales	Equipo De Comunicación	Informaciones Ante Un DRP	Todo El Año	Semanal
		Estadística De Ocurrencia De Catástrofes Naturales		
Propagación De Texto, Video, Audio	Equipo De Comunicación	Informaciones De Un DRP	Todo El Año	Semanal
		Catástrofes Naturales Mas Frecuentes		
		Políticas De Manejo De Crisis		
		Casos De Éxito Y Fracasos Sobre DRP		
Entrenamientos Y Capacitación Sobre El Plan	RRHH	Manejo De Crisis	25 de Junio al 25 de Agosto	2 Horas Cada Sección
		Manejo De Incendios		
		Comunicación Al Cliente Ante Una Crisis		
Asignación De Equipo	Equipo De Manejo De Crisis	Asignación De Equipo Por Pisos Ante Un Incendio	1 de Abril	-
		Asignación De Equipo Por Pisos Ante Un Terremoto		
		Asignación De Equipos De Comunicación Ante Crisis		
		Capacitación De Equipos Por Funciones A Realizar		

Capítulo IX

Plan De Comunicación Ante Incidentes Y Crisis

9.1 Plan De Comunicación Ante Incidentes Y Crisis

Para la correcta implementación de un DRP es necesario contar con un adecuado plan de comunicación ante incidentes y crisis para evitar que la incertidumbre se apodere del personal y de los equipos de trabajos anteriormente designados. Cuando un incidente o crisis se presentan se pueden generar olas de desinformación e inseguridad, a esto se suman otros actores que persiguen obtener constante información sobre la situación lo que genera mucha presión sobre los involucrados. Algunos de los actores son: El gobierno, organizaciones del mismo sector comercial o competencia, etc.

El incorrecto manejo de la comunicación ante incidentes y crisis puede provocar serios daños a la imagen organizacional, negocio y reputación, así también puede ocasionar una sensación de incomprensión y decepción interna y externamente.

9.1.1 Objetivo

Con la elaboración del plan de comunicación ante incidentes y crisis se pretende precisar los procedimientos y funciones a realizar ante la ocurrencia de un desastre o evento no programado que afecte al MINERD.

9.1.2 Definiciones

A continuación se definen los términos crisis e incidentes con el objetivo de brindar un mayor entendimiento sobre cada uno:

Crisis: es un cambio brusco o una modificación importante en el desarrollo de algún suceso. Dichas alteraciones pueden ser físicas o simbólicas.[9]

Incidente: Un incidente es todo aquello que se interpone en el transcurso normal de una situación o de un evento.[10]

9.2 Ciclo de Vida de Comunicación ante Crisis

En un momento de crisis tanto los miembros de los equipos del plan de recuperación ante desastres como los empleados comunes del MINERD y personas externas pueden entrar en un estado en un estado de descontrol e inestabilidad. Para evitar esto se procederá a apoyarse en el ciclo de comunicación ante crisis:

9.2.1 Pre-crisis

Los objetivos de comunicación durante la fase anterior a la crisis son las siguientes:

- Etapa de preparación
- Fomentar las alianzas
- Desarrollo de recomendaciones de consenso
- Los mensajes de prueba

[9] "Definición de", Encontrado 26 de marzo 2012. En la world wide web: http://definicion.de/crisis/

[10] "Definición ABC", Encontrado el 26 de marzo 2012. En la world wide web: http://www.definicionabc.com/derecho/incidente.php

9.2.2 Inicio de crisis

Los objetivos de comunicación durante la fase inicial son las siguientes:

- Reconocer el evento con la empatía.
- Explicar e informar al público, en términos más sencillos,..
- Establecer la organización / credibilidad portavoz.
- Impartir cursos de acción de emergencia (incluyendo cómo / dónde conseguir más información).
- Se comprometen a las partes interesadas y del público a la comunicación continua.

La simplicidad, la credibilidad, la verificabilidad, coherencia, y el recuento de velocidad en la comunicación en las fases iniciales de una emergencia. La fase inicial de una crisis se caracteriza por la confusión y el interés mediático. La información es por lo general incompleta, y los hechos están dispersos.

9.2.3 Mantenimiento de crisis

Los objetivos de comunicación durante la fase de mantenimiento crisis son como sigue:

- Ayudar a las personas con mayor precisión a entender sus propios riesgos.
- Proporcionar información básica y abarca a aquellos que lo necesitan. (¿Cómo pudo suceder esto?).

- ¿Ha sucedido esto antes? ¿Cómo puedo evitar que esto vuelva a ocurrir? ¿Voy a estar bien en el a largo plazo, se puedo recuperar?
- Para obtener la comprensión y el apoyo a planes de respuesta y recuperación.
- Escuche la información de los interesados y el público, y corregir la información errónea.
- Explicar las recomendaciones de emergencia.
- Potenciar el riesgo / beneficio de la toma de decisiones.

Mientras evoluciona la crisis, se debe de anticipar el sostenido interés de los medios y el escrutinio público. Desarrollos inesperados de rumores y la desinformación que puede imponer exigencias adicionales de los medios sobre la organización de los comunicadores.

9.2.4 Resolución de crisis

Los objetivos de comunicación para la fase de resolución son los siguientes:

- Mejorar la respuesta adecuada del público en futuras situaciones de emergencia similares a través de la educación.
- Examinar honestamente los problemas y contratiempos, y luego reforzar lo trabajado en la recuperación y los esfuerzos de respuesta.
- Persuadir al público para apoyar las políticas públicas y la asignación de recursos.
- Promover las actividades y capacidades de la organización

9.3 Evaluación

Cuando se supere la crisis, evaluar el desempeño del plan de comunicación, documentar las lecciones aprendidas y determinar las acciones específicas para mejorar los sistemas de crisis o el plan de crisis.

El grupo de comunicación Burson - Marsteller[11] maneja un decálogo de comunicación de crisis que puede ser de utilidad para el personal del MINERD ante cualquier desastre:

1. **No especular**. Las primeras horas de una crisis se caracterizan por la escasez de información y la poca fiabilidad de los datos. Debe informarse sobre lo que se sabe y sobre lo que se está haciendo para responder a la situación, pero no aventurar hipótesis que no se sostengan con datos. Pero no especular no impide que otros lo hagan. Ante rumores o informaciones erróneas hay que responder rápida y ponderadamente.
2. **No aplicar una "cerrojo informativo"**. Aunque en principio parezca contradictorio con el consejo anterior, las fuentes "oficiales" en una crisis –la empresa o entidad que la sufre o que tiene la responsabilidad de su gestión—deben ser asequibles permanentemente para los medios de comunicación. Es mejor decir "no hay información nueva" que "no hay información". Si las fuentes inmediatas no dan información, los medios la buscarán con otros interlocutores.

[11] "Blog de Andrés Cetta", Encontrado el 26 de marzo 2012. En la world wide web: https://andresmkt.wordpress.com/2012/02/18/decalogo-de-la-comunicacion-de-crisis/

3. **No mentir**. Nunca. Jamás. Si, inadvertida o accidentalmente, se ha dado una información errónea, tomar rápidamente las medidas para corregirla.
4. **Dar la cara y atender al plano emocional** que desencadenan los hechos entre los afectados. Mostrar preocupación, interés y empatía no significa asumir responsabilidades ni aumenta el riesgo de posteriores demandas judiciales. Los afectados –y los medios y sus audiencias— quieren ver a personas "con cara y ojos". Cuando no es así, la sensación que se transmite es nefasta.
5. **No intentar impedir el acceso de los medios de comunicación** al lugar de los hechos y restringir este acceso solo en aras de la seguridad de los periodistas y la facilidad de maniobra de los equipos de emergencia.
6. **Establecer**, cuando la situación lo requiera, **canales de comunicación directa con afectados**, empleados, familiares y otros grupos a través de líneas telefónicas 900 atendidas por personal cualificado, sitios web, puntos de información sobre el terreno, etc.
7. **Compartir** regularmente la **información** de que se dispone **con otras entidades** relacionadas con la crisis (autoridades, servicios de emergencia, etc.) que también puedan ser fuente para los periodistas para limitar el riesgo de contradicciones informativas.
8. **Mantener informados**, cuando es el caso, a empleados, proveedores, clientes…
9. **No eludir responsabilidades ni señalar culpables**, lo cual NO significa asumir responsabilidades que incumben claramente a otros.

10. **No limitar el esfuerzo de comunicación a la fase “activa” de una crisis**. Pasada ésta, suele quedar un gran camino por recorrer para recuperar la confianza de clientes, consumidores, vecinos, etc.

9.4 Desarrollo del Plan de Comunicación ante Incidentes y Crisis

Para el desarrollo de este plan el papel del equipo de manejo de crisis será preponderante dado que sobre este descansan las responsabilidades de decisión y supervisión, antes, durante y post de puesta en marcha del plan.

Los miembros y funciones del equipo de manejo de crisis fueron definidos anteriormente en el capítulo 6 específicamente en el acápite 2.1. No obstante, el comité tiene la potestad de agregar o invitar miembros según entiende pertinente.

9.4.1 Agenda de reuniones

El comité se deberá de reunirse cada 4 meses de manera programada pero también deberá de hacerlo en sesiones extraordinarias según sea necesario o se entienda.

9.4.2 Invitados externos al comité en reuniones

El comité podrá ponderar la asistencia a reuniones de algunos actores externos al equipo con, algunos de estos pueden ser:

- Proveedores o suplidores
- Empleados de posiciones claves
- Medios de comunicación

9.4.3 Asignación de recursos

Con el objetivo de lograr el adecuado desenvolvimiento del personal al momento de activación del DRP el MINERD deberá suministrar los recursos necesarios. Algunos de estos son:

- Personal
- Vehículos
- Recursos financieros
- Equipos de infraestructura
- Entre otros.

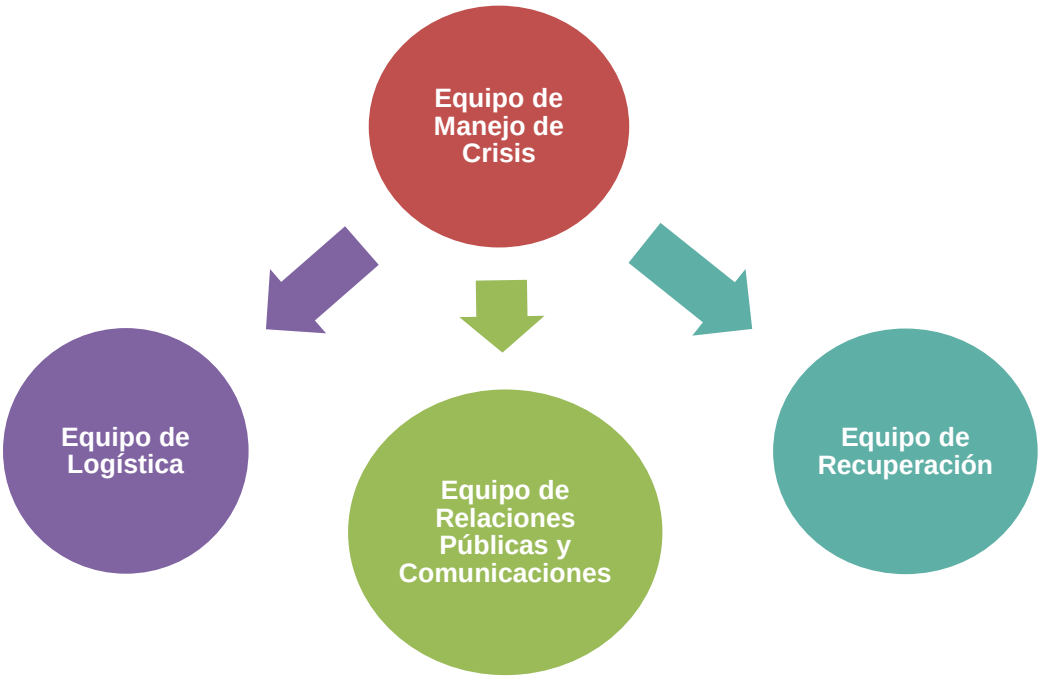
Para esto se apoyará en el equipo de logística supervisado por el equipo de manejo de crisis.

9.4.4 Definición de vocero

El vocero deberá ser definido por el comité de manejo de crisis conjuntamente con el equipo de relaciones públicas. Esta persona será elegida por la mayoría de votos de ambos equipos, dicha mayoría se define como el 50% o más.

9.4.5 Árbol de llamadas

El árbol de llamada se puede definir como un tipo de matriz que presenta el orden de contactos a gestionar al momento de que se presente un incidente para evitar contratiempos. En el momento que se presenta un incidente se define el siguiente árbol de llamadas con los grupos a contactar a la brevedad:



9.4.6 Contactos de Emergencia

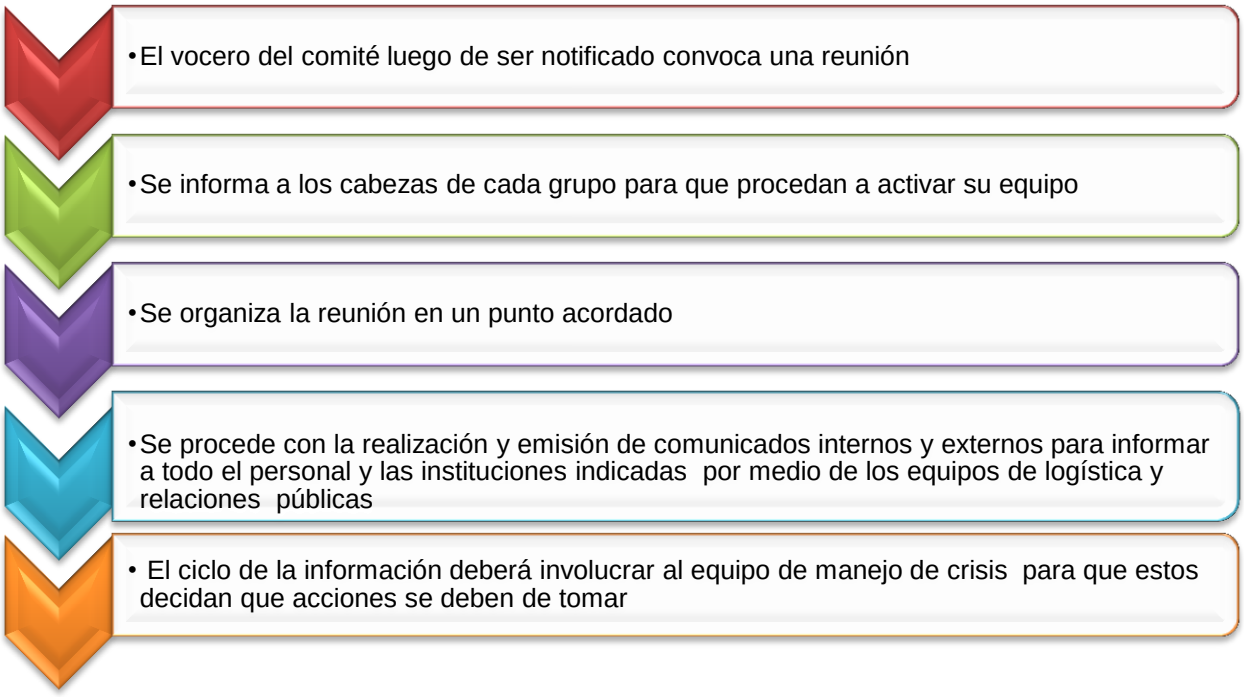
Organización	Teléfono	Aeropuertos y Servicios:	Teléfono
Emergencia	911	Las Américas	(809) 549-0450
Defensa Civil	(809) 682-1749	Puerto Plata	(809) 586-0331
Policía Nacional	(809) 682-2151	La Romana	(809) 813-9000
Meteorología	(809) 788-1122	Punta Cana	(809) 959-2376
Bomberos	(809) 682-2000	Barahona	(809) 524-4144
CAASD	(809) 562-3500	EDE Este	(809) 788-2373
Dirección Nac. De Emerg.	(809) 566-6648	Central	(809) 596-1099
Cruz Roja Dominicana	(809) 682-4545	ONAMET	(809) 788-1122

9.4.7 Procedimiento para el manejo de crisis

Para el manejo de cualquier incidente y crisis en el momento que se presenten se deben de realizar los siguientes pasos inmediatamente:

1) Recolección de información
2) Establecer las circunstancias y escenarios y la relación
3) Determinar el orden de los eventos y sus consecuencias

A continuación mostramos una secuencia de las acciones a tomar:



CONCLUSIÓN

El Plan de Recuperación ante Desastre (DRP) presentado para el Ministerio de Educación (MINERD) fue adaptado a las necesidades que este reflejó durante los procesos de investigación. Identificando las amenazas y riesgos más comunes, que podrían afectar las instalaciones, así como también los procesos críticos que se verían afectados ante la insurgencia de cualquier evento.

Por lo tanto, se seleccionó y desarrolló una estrategia basada en la recuperación efectiva de los procesos críticos que son apoyados por los diferentes sistemas de información que tiene el MINERD, además se establecieron los parámetros y tiempos clave para el mantenimiento del plan, y una adecuada estrategia para comunicar al cliente interno y externo de la institución antes, durante y después de un evento no programado o crisis.

En fin, un DRP debe de ser parte esencia de todas las organizaciones públicas y privadas, ya que, este se utiliza con la finalizada de garantizar las operaciones de los procesos apoyados en tecnología ante cualquier problemática de origen humano o natural.

BIBLIOGRAFIA

- Harris, Shon. (2005). CISSP, Business Continuing Planning. 3th ED, McGraw Hill/Osborne third edition. USA.

- Hansche, Susan. Berti, John. Hare, Chris. (2003). Official, (ISC) Guide To The CISSP Exam. CRC, Press. Boca Raton, Florida.

- Gregory, Peter. (2008). IT Disaster Recovery Planning For Dummies. Wiley Publishing, Inc. Hoboken, NJ. USA.

- Disaster Recovery Planning. Universidad de Toronto, Technology Services. Encontrado 25 enero 2012. En la World Wide Web: http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm

- Crisis and Emergency Risk. Centers for Disease Control and Prevention. Encontrado el 15 de marzo 2012. En la World Wide Web: http://www.au.af.mil/au/awc/awcgate/cdc/cerc_book.pdf

- Disaster Recovery Planning – Process & Options (2001), Comprehensive Consulting Solutions, Inc. (White Paper). Encontrado 15 enero 2012. En la World Wide Web: http://www.comp-soln.com/DRP2_whitepaper.pdf

- Análisis de Riesgos de Desastres y vulnerabilidades en la República Dominicana, marzo 2009. Encontrado 03 marzo 2012. En la World Wide Web:http://ec.europa.eu/echo/files/funding/opportunities/interest_dipecho 7_Rep_Dominicana.pdf

- Diccionario de la Real Academia Española. Consultado última vez, 23 marzo 2012. En la World Wide Web: http://www.rae.es/rae.html

- Ministerio de Educación de la República Dominicana. Consultado última vez, 10 marzo 2012. En la World Wide Web: http://www.see.gob.do/Pages/Planificacion/planificacion.aspx

GLOSARIO

TIC: Tecnologías de Información y Comunicación.

Hardware: Conjunto de los componentes que integran la parte material de una computadora.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Tecnología: Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico.

IT / TI: *(Information Tecnology),* Tecnología de la Información

Sistema: Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto.

Hacking: Acción del Hacker.

Hacker: Una persona que disfruta explorando los detalles de sistemas programables y el estiramiento de sus posibilidades, a diferencia de la mayoría de los usuarios, que prefieren aprender sólo lo mínimo necesario.

Anonymous: representa el concepto de muchos usuarios de la comunidad online y offline de forma simultánea ya existentes, como el cerebro de un anárquico, global digitalizada.

Denegación de Servicio (DoS): *(Denial of Services Attack)* Ataque de denegación de servicio, es un intento de hacer que un recurso de equipo o la red no esté disponible para sus usuarios.

Router: es un dispositivo que envía paquetes de datos entre redes de computadoras, la creación de una interconexión de redes.

Switch: es un dispositivo de red informática que conecta segmentos de red o dispositivos de red.

Servidores: un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes.

Cable UTP: *(Unshielded Twisted Pair)* Abreviatura de par trenzado no blindado, un tipo popular de cable que consta de dos cables de par trenzado sin blindaje alrededor de la otra.

Iptables: es un programa o aplicación que permite a un administrador del sistema configurar las tablas proporcionadas por el servidor de seguridad.

UPS: *(Uninterruptible Power Supply),* sistema de alimentación ininterrumpida, es un aparato eléctrico que proporciona energía de emergencia a una carga cuando la fuente de alimentación de entrada, por lo general la red eléctrica, falla.

Power Supply: es un dispositivo que suministra energía eléctrica a una o más cargas eléctricas.

RAM: *(Random Access Memory),* es una forma de almacenamiento de datos para computadoras y dispositivos eléctrico.

Rack: es un marco estandarizado o recinto para el montaje de los módulos de múltiples equipos computacionales.

KVM Switch: es un dispositivo de hardware que permite al usuario controlar múltiples ordenadores desde un monitor de video con teclado y mouse.

In house: es un término que significa “dentro de casa” pero en el contexto informático se refiere que un software fue creado y consumido por la misma organización.

Proxy: es un servidor (un sistema informático o una aplicación) que actúa como intermediario en las peticiones de los clientes en busca de recursos desde otros servidores.

SharePoint: es una plataforma de aplicación Web desarrollada por Microsoft. Por lo general asociados a la gestión de contenidos web y sistemas de gestión de documentos.

Joomla: es un sistema de gestión de contenido para la publicación de contenidos en internet e intranets.

Lync: Es un cliente de mensajería instantánea y comunicaciones (voz y video) destinado para empresas.

Roadmap: Es un plan que coincide con las metas a corto y largo plazo con soluciones tecnológicas específicas para ayudar a alcanzar esas metas.

Report Server: Servidor de Reportes. El lugar donde se procesa y almacena reportes de aplicaciones o software.

Network: Red de Computadoras, es una colección de componentes de hardware y ordenadores interconectados por canales de comunicación que permiten compartir recursos e información.

Firewall: es un dispositivo o conjunto de dispositivos diseñados para permitir o denegar las transmisiones de red basados en un conjunto de normas y se utiliza con frecuencia para proteger las redes contra el acceso no autorizado, al tiempo que permite las comunicaciones legítimas de pasar.

Mirror Site / Mirroring: En informática, un espejo es una copia exacta de un conjunto de datos. En Internet, un sitio espejo es una copia exacta de otro sitio de Internet.

Frame Relay: es un estándar de tecnología de red de área que especifica las capas de enlace físico y lógico de los canales de telecomunicaciones digitales utilizando una metodología de conmutación de paquetes.

Cloud Computing: es la entrega de la informática como un servicio más que un producto, mediante el cual los recursos compartidos, software e información se proporcionan a los ordenadores y otros dispositivos como una utilidad (como la red eléctrica) en una red (generalmente Internet).

Windows Azure: es una plataforma de computación en la nube Microsoft utiliza para construir, hospedar y escalar las aplicaciones web a través de los centros de datos de Microsoft.

ANEXOS

Anexo I

UNIVERSIDAD APEC

DECANATO DE INGENIERÍA E INFORMÁTICA

ESCUELA DE INFORMÁTICA

Plan de recuperación ante desastres aplicado al área de tecnología del Ministerio de Educación de la República Dominicana (MINERD) en el periodo Enero-Abril 2012.

Sustentantes:

Gregorys José Sosa González	2006-0576
Jhancarlo Veras Chalas	2006-1486
Yamayco Sánchez Núñez	2007-0155

Asesores:

Ramón Gómez

Antonio Calderón

Anteproyecto de la Monografía para Optar por el Título de:

Ingeniero en Sistemas de Información

Distrito Nacional, Republica Dominicana

2012

PLAN DE RECUPERACIÓN ANTE DESASTRES APLICADO AL ÁREA DE TECNOLOGÍA DEL MINISTERIO DE EDUCACIÓN DE LA REPÚBLICA DOMINICANA (MINERD) EN EL PERIODO ENERO-ABRIL 2012.

ÍNDICE

1. SELECCIÓN DEL TÍTULO Y DEFINICIÓN DEL TEMA

Plan de recuperación ante desastres aplicado al área de tecnología del Ministerio de Educación de la República Dominicana (MINERD) en el periodo Enero-Abril 2012.

1.1 DEFINICIÓN DEL TEMA

En este trabajo de grado se plantea un plan de recuperación ante desastres (DRP) que garantice la continuidad de los sistemas tecnológicos, los cuales sirven como base o soporte a los procesos críticos del Ministerio de Educación de la República Dominicana (MINERD). Los procesos antes mencionados apoyan a su vez los planes de desarrollo de la educación en la República Dominicana, debido a esto se procura garantizar la disponibilidad, integridad y confiabilidad de la información de los mismos luego de un incidente, catástrofe o evento no programado.

2. PLANTEAMIENTO DEL PROBLEMA

En el mundo moderno, tecnológico y automatizado, la información se ha convertido en un activo de sumo valor para las empresas sin importar el tamaño o la actividad a la que esta se dedica. No obstante, la mayoría de estas no prestan la suficiente importancia, ni el cuidado adecuado a los sistemas que garantice la continuidad de los procesos de negocios ante cualquier catástrofe natural o evento no programado.

En la actualidad los diferentes cambios atmosféricos y movimientos telúricos como fueron: El tsunami de Indonesia (2004), terremoto y tsunami de Japón (2011), terremoto de Chile (2011), terremoto de Haití (2011), entre otros, mantienen en constante amenaza o riesgo la estabilidad empresarial y sus sistemas informáticos. Esto obliga a las empresas tanto a nivel nacional como internacional a pensar en como salvaguardar su información para que sus operaciones se vean lo menos afectadas posibles en caso de un suceso.

Los fenómenos naturales no son los únicos riesgos o amenazas que enfrentan las empresas dado que existen otras como son: Crackers, hackers, virus, interrupciones eléctricas, sabotajes, incendios, fallas estructurales, inundaciones, etc.

Según datos extraídos de la cámara de comercio de Londres[12] las consecuencias de no contar con un plan de continuidad de negocio apropiado pueden ser graves para las empresas al momento de suceder una catástrofe o situación inesperada. A continuación se presentan las informaciones antes mencionadas:

- ✓ El 43% de las organizaciones después de un accidente no podrán continuar sus operaciones viéndose obligadas a cerrar.

[12] SMALL COMPANIES MUST IMPLEMENT DISASTER CONTINGENCY PLANS NOW – LONDON CHAMBER OF COMMERCE. Encontrado 10 enero 2012. En la World Wide Web: http://www.londonchamber.co.uk/lcc_public/article.asp?id=1&did=&aid=1187&st=disaster&oaid=

- ✓ El 80% tendrán que hacerlo en menos de 13 meses.
- ✓ El 53% de los clientes de estas organizaciones no recuperarán las pérdidas causadas por los daños derivados.
- ✓ El 50% se verán forzadas a cerrar antes de cinco años después del desastre.

La República Dominicana no escapa a las amenazas antes expuesta ya sean de orden natural o evento no programado esto por su posición geográfica y por las faltas de normativas o regulaciones que exijan una mayor y mejor supervisión a las empresas respecto al manejo de su información.

En el área de tecnología del Ministerio de Educación de la República Dominicana ha sido posible observar que no cuentan con una documentación que avale un plan de continuidad de negocios que garantice una continuidad de los sistemas que son soporte al plan de educación y toda la información que tiene actualmente.

En el Ministerio de Educación de República Dominicana (MINERD) ha sido posible observar que siendo el corazón central de la educación básica e intermedia del país no cuenta con un plan de recuperación ante desastres que permita garantizar la continuidad de las operaciones del área de tecnología que es uno de lo mas importantes soportes de los planes de educación que cuenta.

3. OBJETIVOS DE LA INVESTIGACIÓN

3.1 OBJETIVO GENERAL

- ✓ Desarrollar un Plan de Recuperación ante Desastres (DRP) que garantice la continuidad de las operaciones tecnológicas del área de tecnología del Ministerio de Educación de República Dominicana (MINERD).

3.2 OBJETIVOS ESPECÍFICOS

- ✓ Identificar las vulnerabilidades, riesgos y procesos críticos existentes en el área de tecnología del MINERD, mediante la evaluación de los análisis de riesgo e impacto del negocio.
- ✓ Evaluar el impacto de una eventual falla en el funcionamiento de los sistemas de información que soportan los procesos críticos del MINERD.
- ✓ Diseñar un conjunto de estrategias que permitan la restauración de los sistemas informáticos que soportan los procesos críticos para el MINERD dentro del área de tecnología en el tiempo establecido por la directiva del mismo.
- ✓ Garantizar la disponibilidad, confiabilidad e integridad de la información al momento de puesta en marcha del Plan de Recuperación ante Desastres (DRP).
- ✓ Documentar el Plan de Recuperación ante Desastres y los responsables de cada una de las acciones a tomar en caso de cualquier eventualidad que se presente.

- ✓ Definir posibles escenarios de desastres para el área de tecnología del MINERD.

4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

4.1 JUSTIFICACIÓN TEÓRICA

Esta investigación busca mediante la aplicación de la teoría, observación y los procesos de continuidad de negocio planificar, elaborar y presentar un Plan de Recuperación ante Desastres al área de tecnología del Ministerio de Educación de República Dominicana (MINERD) con el objetivo de garantizar la continuidad de los planes de educación que están soportados por equipos tecnológicos y sistemas de información ante cualquier situación de desastre.

4.2 JUSTIFICACIÓN METODOLÓGICA

Para lograr el cumplimiento de los objetivos del estudio de investigación se emplearán diversas técnicas que permitan identificar los riesgos y amenazas a los cuales se enfrenta el área de tecnología del Ministerio de Educación de República Dominicana (MINERD), analizando el impacto provocado por una posible salida de funcionamiento de sus sistemas de información en sus operaciones. Adicionalmente se utilizarán las siguientes técnicas: cuestionarios y entrevistas que permitan ver las características cualitativas y cuantitativas de la investigación.

4.3 JUSTIFICACIÓN PRÁCTICA

Debido a que este proyecto es un requisito reglamentario para obtener el título de grado de Ingeniería en Sistemas de Información (ISI) el principal objetivo es aprobar el curso de monográfico o monografía con una calificación excelente.

También se espera aportar un Plan de Recuperación ante Desastres (DRP) que garantice la continuidad de los sistemas mantenidos por el área de tecnología y que soportan el plan de educación del Ministerio de Educación de República Dominicana (MINERD) en caso de cualquier desastre o evento programado.

5. TIPOS DE INVESTIGACIÓN

Para el desarrollo del trabajo de grado se utilizarán los siguientes tipos de investigación:

a) **Descriptiva:** Es un tipo de estudio que sirve para analizar cómo se manifiesta el objeto de investigación y sus componentes. Este será utilizada para el desarrollo del trabajo de grado debido a que se detectaran las diferentes características negativas que presenta el área de tecnología del Ministerio de Educación de República Dominicana (MINERD), como así también se utilizaran técnicas especificas en la recolección de información como son las entrevistas, observación, y cuestionario, que ayudaran a identificar datos relevantes para la investigación.

b) **Explicativa:** Es un tipo estudio que busca encontrar las razones o causas que ocasionan cierto fenómenos. Este será utilizado debido a que se realizaran pruebas minuciosas que expliquen de forma clara y precisa las hipótesis plantadas. Así como también se indicaran las causas y resultados que expresen los hechos planteados, mediante un análisis, síntesis e interpretación de la información recolectada.

c) **Documental:** Es un tipo de estudio que busca indagar las causas en que generaron o generaran ciertos fenómenos. Este será utilizado en el trabajo de investigación debido a que como los documentales que son un tipo de investigación que utiliza estés tipo de estudio, recolectaremos una serie de información con la finalidad de determinar los efectos o impacto que produciría la falta de un plan de recuperación ante desastre (DRP) en el Ministerio de Educación de República Dominicana (MINERD).

6. MARCOS DE REFERENCIA

6.1 MARCO TEÓRICO

“El objetivo de un plan de recuperación de desastres es minimizar el efecto de un desastre y tomar las acciones necesarias para asegurar que los recursos, el

personal, y que los procesos de negocios estén habilitados y disponibles en el menor tiempo posible"[13].

"El plan de recuperación de desastres se refiere a la inmediata restauración de los procesos críticos computacionales y las operaciones de la red después de un desastre natural o por intervención humana dentro de un marco de tiempo definido. Una organización documenta como responderá a los desastres y restaura las funciones de negocios críticos dentro de un período de tiempo determinado; minimiza el número de pérdidas; y repara o remplaza lo primordial dentro de la localidad para restaurar el procesamiento de datos"[14].

"Un proyecto de recuperación de desastres no se puede completar en una semana o un mes. En muchos sentidos, un DRP no se completa, el plan debe ser probado y actualizado al menos una vez al año, si no es con más frecuencia. Un plan que no se adapta al ritmo de los cambios en la organización, es un desastre en sí misma, proporcionando una falsa sensación de seguridad. Por lo tanto, mientras se puede tener un plan de trabajo diario, el

[13]HARRIS, Shon. (2005). CISSP, Business Continuing Planning. (pp. 691). USA, McGraw Hill/Osborne third edition.
[14] HANSCHE, Susan. BERTI, John. HARE, Chris. (2003). Official, (ISC) Guide To The CISSP Exam. (pp. 663). Boca Raton, Florida. CRC, Press.

proyecto tiene estar actualizado para asegurar que el plan funcione siempre que fuere requerido”[15].

La implementación de un DRP siempre debe tener como objetivo la restauración de la tecnología que soporta los procesos críticos. Este por lo general, conlleva una planificación estructurada que necesita ser documentada, probada y actualizada. Además, es importante que el mismo involucre al personal para que en caso de una eventualidad el plan pueda ejecutarse satisfactoriamente, recuperando los recursos y procesos en el menor tiempo posible.

6.2 MARCO CONCEPTUAL

Desastre: Desgracia grande, suceso infeliz y lamentable.

Plan de recuperación ante desastres (DRP): Es una guía de pasos a seguir en una organización ante un evento o desastre con el objetivo de restablecer los procesos tecnológicos críticos del negocio en el menor tiempo posible y con la mínima perdida de datos.

Contingencia: Posibilidad de que algo suceda o no suceda.

[15] Disaster Recovery Planning – Process & Options, Comprehensive Consulting Solutions, Inc. (White Paper). PP. 3. Encontrado 15 enero 2012. En la World Wide Web: http://www.comp-soln.com/DRP2_whitepaper.pdf

Riesgo: Una acción o evento que causa incertidumbre y que de ocurrir produce consecuencias adversas.

Probabilidad: En un proceso aleatorio, razón entre el número de casos favorables y el número de casos posibles.

Evaluar: Estimar, apreciar, calcular el valor de algo.

Impacto: Conjunto de posibles efectos negativos o positivos sobre la codificación de un entorno cualquiera.

Vulnerabilidad: Característica o situación puntual de un activo que puede ser aprovechada /explotada por una amenaza.

Continuidad: Acción de Seguimiento o restauración de alguna actividad.

Interrupción: Acción de detener un proceso o su restauración.

Control: Medidas/acciones para modificar el riesgo. Incluye cualquier proceso, política, dispositivo, práctica u otra acción que modifique un riesgo.

Centro de procesamiento datos (Datacenter): Es una ubicación en la cual se encuentran los recursos necesarios para el procesamiento de la información de una organización.

Objetivo de Tiempo de Recuperación (RTO): Es el periodo máximo de tiempo que un proceso de negocio puede estar fuera de servicio antes de ser reiniciado.

Objetivo de punto de recuperación (RPO): Es la cantidad máxima de pérdida de datos que una organización puede tolerar ante un desastre que interrumpa los procesos críticos del negocio.

Tiempo de Recuperación Actual (RTA): Es el periodo de tiempo que el soporte tecnológico puede recuperar la infraestructura del negocio.

Equipo de respuesta en emergencia (ERT): Es el equipo de personas dentro de la organización que pueden ser contactadas a cualquier hora del día o de la noche, cuando ocurra un desastre.

6.3 MARCO ESPACIAL

Esta investigación o trabajo de grado será realizada en el área de tecnología, formalmente, la Dirección General Tecnología de Información y Comunicaciones del Ministerio de Educación de República Dominicana, cede central, el cual está ubicado en la avenida Máximo Gómez esquina Santiago, #02 Gazcue D.N., República Dominicana.

6.4 MARCO TEMPORAL

La investigación antes mencionada será realizada en el periodo que comprende los meses de Enero-Abril del año 2012.

7. MÉTODOS, PROCEDIMIENTOS Y TÉCNICAS UTILIZADAS EN LA INVESTIGACIÓN

7.1 MÉTODO

Las metodologías que se utilizará para este trabajo de grado son:

a) Método Observación

Se utilizara este método debido a que se realizarán meticulosas observaciones de las problemática planteada en nuestro caso el impacto que generaría la falta de un plan de recuperación ante desastre en el Ministerio de Educación de República Dominicana (MINERD).

b) Método Inductivo

Se realizará un análisis ordenado, coherente y lógico de las situaciones observadas, el cual tendrá como objetivo confirmar los datos y hechos anteriormente observados.

c) Método Deductivo

Se utilizará este método el cuál será basado en la observación anteriormente realizada con la finalidad de señalar las particularidades del problema planteado.

d) Método de Análisis y Síntesis

Se utilizarán este método debido a que se establecerán las razones de causa y efecto de lo que los factores que provocan la problemática y se realizará una síntesis del análisis realizado.

7.2 PROCEDIMIENTO

Luego de obtener las informaciones recolectadas mediantes los métodos antes mencionados se realizaran las siguientes actividades:

a) Descripción de la organización.
b) Análisis de riesgo
c) Análisis de impacto
d) Establecimiento de las estrategias de recuperación
e) Desarrollo de un plan de recuperación ante desastre (DRP)
f) Realización de un plan de concientización ante crisis.
g) Realización de informe final del proyecto.

7.3 TÉCNICA

Las técnicas utilizadas para la recolección de información de este trabajo de grado serán:

- ✓ **La entrevista:** Se utilizará esta técnica para la recolección o extracción de la información que será utilizada para el desarrollo del trabajo de investigación. Dichas entrevista serán realizadas a todo el personal

considerado clave o necesario, esto incluyen directores, supervisores, técnicos involucrados y personal administrativo.

- ✓ **Cuestionarios:** Son un conjunto de preguntas, preparadas cuidadosamente, sobre los hechos y aspectos que interesan en una investigación, para que sea contestado por la población o su muestra. En este sentido se utilizará esta técnica con el objetivo de obtener el conocimiento sobre el todo el entorno de trabajo, como así también de las operaciones que son realizada en todo el entorno del MINERD, con la finalidad de que el mismo sea utilizado en el trabajo de investigación.

8. TABLA DE CONTENIDO

Capítulo V Estrategias De Recuperación

Capítulo VI Desarrollo Del Plan De Recuperación Ante Desastres

Capítulo VII Diseño De Pruebas Y Mantenimiento Del Plan

Capítulo VIII Programa De Capacitación Y Concientización Del Plan

Capítulo IX Plan De Comunicación Ante Incidentes Y Crisis

9. FUENTES DE INFORMACIÓN

- Harris, Shon. (2005). CISSP, Business Continuing Planning. 3th ED, McGraw Hill/Osborne third edition. USA.

- Hansche, Susan. Berti, John. Hare, Chris. (2003). Official, (ISC) Guide To The CISSP Exam. CRC, Press. Boca Raton, Florida.

- Gregory, Peter. (2008). IT Disaster Recovery Planning For Dummies. Wiley Publishing, Inc. Hoboken, NJ. USA.

- Disaster Recovery Planning. Universidad de Toronto, Technology Services. Encontrado 25 enero 2012. En la World Wide Web: http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm

- Disaster Recovery Planning – Process & Options (2001), Comprehensive Consulting Solutions, Inc. (White Paper). Encontrado 15 enero 2012. En la World Wide Web: http://www.comp-soln.com/DRP2_whitepaper.pdf

Anexo II

Nombre	
Departamento o área	
Puesto o título	
Correo electrónico	
Fecha	

En los siguientes cuadros complete la información solicitada según aplique para los procesos y subprocesos que usted supervisa:

Nombre de proceso	Subprocesos	Descripción	Frecuencia de uso (Diario/Semanal/ Mensual)	Puesto o nombre de responsable

Nombre de proceso	Periodo de tiempo máximo permitido (x)		Nombre de proceso	Cantidad de data tolerable a perder (x)	
	Menos de 4 horas sin servicio	☐		Menos de 4 horas de información	☐
	4-8 horas sin servicio	☐		4-8 horas de información	☐
	8-24 horas sin servicio	☐		8-24 horas de información	☐
	1-3 días sin servicio	☐		1-3 días de información	☐
	3-5 días sin servicio	☐		3-5 días de información	☐

Indique cuáles son los factores de costos están asociados con la interrupción del servicio en el área o departamento:		
Factores de costos intangibles	**Descripción**	**Ingrese el costo estimado**
Reducción o efecto sobre el servicio al cliente	Estos pueden incluir niveles reducidos o terminados de servicio, información que no está disponible cuando los clientes llamen, los clientes no pueden acceder a la información en el sitio Web, etc. Esto podría ser difícil de estimar en la mayoría de los casos.	
Reducción de productividad	Estos podrían incluir la implicación para otros departamentos o áreas si el proceso no está disponible. También abarca los costos de empleados que son productivos mientras el proceso no está disponible.	
Reducción en la confianza o problemas de imagen	Estas son amenazas que podrían tener un enorme impacto en el negocio. Ejemplos: Un fallo de seguridad, virus, publicación de data no confiable o integridad de la información	
	Total RD$	

Anexo III