

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL



Facultad de Ingeniería en Electricidad y Computación

DESARROLLO DE UN PLAN DE RECUPERACIÓN ANTE
DESASTRES (DRP) PARA LA UNIDAD DE T.I. DE LA
CORPORACIÓN AMCO

PROYECTO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
MAGISTER DE SEGURIDAD INFORMÁTICA APLICADA

AUTORES

JOHN JOSÉ CHAMBA MERA
LUIS IGNACIO DELGADO ÁLVAREZ

GUAYAQUIL - ECUADOR

2017

AGRADECIMIENTO

A Dios, por darme vida y las fuerzas necesarias para alcanzar esta meta que me ayudará a crecer en el aspecto humano y profesional.

A los miembros de mi familia por ser el soporte e inspiración que me permiten culminar el presente trabajo.

A la Escuela Superior Politécnica del Litoral, y principalmente a todos los integrantes que conforman el programa MSIA por toda su ayuda y conocimientos brindados.

Al Ing. Lenin Freire, Director de tesis y Coordinador del programa MSIA, por todo su tiempo y valiosa ayuda.

Muchas Gracias.

John José Chamba Mera.

AGRADECIMIENTO

Agradezco infinitamente a nuestro creador ya que sin él no lo hubiera logrado. A mis padres quienes con su sacrificio y amor me apoyaron en todo momento, a mi esposa quien con mucha paciencia y amor supo esperar y entender las largas horas de ausencia, trabajo y estudio. Gracias a mi madre, gracias a mi esposa por tenerme presente en sus oraciones y por creer en mí.

También agradezco a todas las personas que hicieron posible cumplir con esta importante y anhelada meta, mi director de tesis, gracias por la colaboración brindada

Luis Delgado Álvarez

DEDICATORIA

A mis padres, José y Margarita, por su amor incondicional y apoyo infinito, todo lo que soy se los debo a ellos.

Al amor de mi vida, Andrea Tatiana, por su apoyo, comprensión y aliento para culminar el presente trabajo.

A todas las demás personas que me brindaron su colaboración en esta tan importante meta.

John José Chamba Mera.


Este trabajo está dedicado a mi mamá, papá y esposa. Los pilares fundamentales en mi vida, en ellos tuve apoyo incondicional, rectitud y amor. Gracias familia por incentivar me a terminar esta meta.

Luis Delgado Álvarez


TRIBUNAL DE SUSTENTACIÓN



MG. LENIN FREIRE COBO
DIRECTOR MSIA



MG. LENIN FREIRE COBO
DIRECTOR DE TESIS



MG. NÉSTOR ARREAGA ALVARADO
MIEMBRO PRINCIPAL

DECLARACIÓN EXPRESA

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



JOHN JOSÉ CHAMBA MERA

C. I. 1309882999



LUIS IGNACIO DELGADO ÁLVAREZ

C.I. 1307916724

RESUMEN

El Plan de Recuperación ante Desastres para la Unidad de T.I. de la Corporación AMCO, tiene su origen en los hallazgos encontrados en la última auditoría, en la que menciona la carencia de planes de recuperación de los servicios de T.I. que brinda la Corporación, además del desastre natural ocurrido el 16 de abril de 2016 en la provincia de Manabí.

Debido a esto, el presente trabajo de investigación tiene como fin el desarrollo del Plan de Recuperación para la continuidad de los servicios de T.I. de AMCO, tomando como base el estándar ISO 22301:2012, lo que ayudará a la Corporación al aseguramiento de la disponibilidad de sus servicios de T.I. garantizando la continuidad de sus operaciones.

Para la correcta validación del plan se analizan riesgos y se establecen políticas, estrategias y planes de recuperación para los servicios y aplicativos de T.I. Se realizan pruebas y simulacros para determinar su correcta aplicación, así como acciones correctivas y mejoramiento continuo del Plan.

ÍNDICE GENERAL

AGRADECIMIENTO	i
DEDICATORIA	iii
TRIBUNAL DE SUSTENTACIÓN	iv
DECLARACIÓN EXPRESA	v
RESUMEN.....	vi
ÍNDICE GENERAL	vii
ABREVIATURAS Y SIMBOLOGÍA	xii
ÍNDICE DE FIGURAS.....	xiv
ÍNDICE DE TABLAS.....	xv
INTRODUCCIÓN.....	xvi
CAPÍTULO 1.....	1
GENERALIDADES	1
1.1. Antecedentes	2
1.2. Descripción del problema.....	3
1.3. Alcance	4
1.4. Solución propuesta	5
1.5. Objetivo General	6
1.6. Objetivos Específicos	6
1.7. Metodología	6

CAPÍTULO 2.....	8
MARCO TEÓRICO	8
2.1. Antecedentes (Preámbulo).....	8
2.2. Definiciones Fundamentales	9
2.3. Plan de Recuperación ante Desastres (DRP)	18
2.4. Estándares y Normativas utilizados en los DRP's.	20
2.5. Modelo PDCA.	31
2.5.1. Fase de Planificación (PLAN).....	32
2.5.2. Fase de Realización (DO).....	33
2.5.3. Fase de Verificación (Check).	33
2.5.4. Fase de Ajuste (ACT).....	34
2.6. Selección del estándar a aplicar.....	34
CAPÍTULO 3.....	37
DEFINICIÓN DE LA SITUACIÓN ACTUAL	37
3.1 Descripción del Departamento de T.I.	37
3.2 Organigramas de la empresa y de T.I.	37
3.4. Infraestructura Técnica.....	47
3.5. Aplicaciones.....	48
3.6. Implementación del modelo	49
3.6.1. Fase de Planificación (PLAN).....	50
3.6.2. Fase de Realización (DO).....	50
3.6.3. Fase de Verificación (Check)	51

3.6.4. Fase de Ajuste (ACT).....	52
3.7. Roles y Responsabilidades	52
CAPÍTULO 4.....	62
ANÁLISIS Y DISEÑO DEL PLAN DE RECUPERACIÓN ANTE DESASTRES	62
4.1. Procedimiento para control de documentos y registros	63
4.2. Plan del Proyecto	63
4.3. Procedimiento para identificación de requisitos.....	63
Lista de requisitos legales, normativos y contractuales.....	64
4.4. Política para la recuperación ante desastres.....	64
4.5. Metodología para el análisis del impacto en el negocio.....	64
4.5.1. Cuestionario sobre el análisis del impacto en el negocio –Servicios de Telecomunicaciones.	64
4.5.2. Cuestionario sobre el análisis del impacto en el negocio – Sistemas y aplicativos de AMCO.....	65
4.6. Estrategia de recuperación ante desastres.	65
4.6.1. Lista de actividades.....	65
4.6.2. Prioridades de recuperación para las actividades	65
4.6.3. Objetivos de tiempo de recuperación para las actividades.....	66
4.6.4. Ejemplos de escenarios de incidentes disruptivos	66
4.6.5. Plan de preparación para la continuidad de los servicios de TI.	66

4.6.6. Estrategia de recuperación - Disponibilidad de los servicios de telecomunicaciones.....	66
4.6.7. Estrategia de recuperación - Disponibilidad de Sistemas y aplicativos de AMCO:	67
4.7. Plan de recuperación ante desastres.	67
4.7.1. Plan de respuesta a los incidentes.....	67
4.7.2. Registro de Incidentes.	67
4.7.3. Ubicaciones para la continuidad de las operaciones.....	68
4.7.4. Plan de Transporte.	68
4.7.5 Contactos Claves.....	68
4.7.6. Plan de recuperación – Servicio de telecomunicaciones.....	68
4.7.7. Plan de recuperación – Servicio de sistemas y aplicativos.....	68
CAPÍTULO 5.....	70
ESQUEMA DE PRUEBAS Y ANÁLISIS DE RESULTADOS DEL DRP.....	70
5.1. Pruebas, mantenimiento y revisión del DRP.	71
5.1.1. Informe de pruebas y verificación.....	71
5.1.2. Plan de mantenimiento y revisión del DRP.....	71
5.1.3. Formulario de revisión postincidente	71
5.2. Plan de capacitación y concienciación.	72
5.3. Procedimiento para auditoría interna.....	72
5.3.1. Programa anual de auditoría interna.....	72
5.3.2. Informe de auditoría interna.	72

5.3.3. Lista de apoyo de auditoría interna.	73
5.4. Minutas de Revisión por parte de la dirección.	73
5.5. Procedimiento para medidas correctivas.....	73
Formulario para medidas correctivas.	73
CAPÍTULO 6.....	74
ANÁLISIS DE RESULTADOS	74
6.1. Inconvenientes durante la ejecución del DRP.	74
6.2. Resultados del modelo aplicado.....	75
CONCLUSIONES Y RECOMENDACIONES	77
BIBLIOGRAFÍA.....	80
GLOSARIO DE TÉRMINOS	84
ANEXOS	87

ABREVIATURAS Y SIMBOLOGÍA

BCM	Business Continuity Management
BCMS	Business Continuity Management System
BIA	Business Impact Analysis
BS.	British Standard
CNEL	Corporación Nacional de Electricidad
CNT	Corporación Nacional de Telecomunicaciones
DRP	Plan de recuperación de desastres
EPR	Empresa por Resultados. Sistema de Planeación Estratégica
ERP	Enterprise Resource Planning. Conjunto de sistemas de Información
IP	Internet protocol (Protocolo de internet).
ISO	International Organization for Standardization
ISP	Internet service providers (Proveedor de servicios de internet).
LAN	Local area network (Red de area local).

RPO	Recovery Point Objective
RTO:	Recovery Time Objective
SGCN	Gestión de la continuidad del negocio.
SGSI	Sistema de Gestión de Seguridad de la Información.
SQL	Structure Query Language
TI	Tecnología de la Información
VPN	Virtual private networks (Redes virtuales privadas).
WAN	Metropolitan area network (Red de area metropolitana).

ÍNDICE DE FIGURAS

Figura 2.1: Sistema de Información	14
Figura 3.1: Estructura orgánica de AMCO	38
Figura 3.2: Estructura Orgánica de TI	39
Figura 3.3: Infraestructura de red y dispositivos de AMCO	48

ÍNDICE DE TABLAS

Tabla 1: Documentos de la Fase de Planificación	33
Tabla 2: Documentos de la Fase de Realización	33
Tabla 3: Fase de Verificación	34
Tabla 4: Fase de Ajuste	34
Tabla 5: Selección del estándar según criterios de selección	36
Tabla 6: Servicios de TI por Departamento.....	43
Tabla 7: Listado de los servicios de TI y su frecuencia de uso.....	44
Tabla 8: Fase de Planificación	50
Tabla 9: Fase de Realización	50
Tabla 10: Fase de Verificación.....	52
Tabla 11: Fase de Ajuste	52

INTRODUCCIÓN

El presente tema de investigación tiene como base el desarrollo de un Plan de Recuperación ante desastres para la unidad de T.I. de la Corporación AMCO con la finalidad de que sea aceptado e implementado por esta empresa y le brinde continuidad a su infraestructura tecnológica que da soporte a las actividades y servicios de la corporación.

El trabajo de investigación está conformado por seis capítulos:

En el capítulo número uno, se detallan las generalidades, antecedentes, descripción del problema, su alcance, así como la solución propuesta y el planteamiento del objetivo general y los objetivos específicos.

En el capítulo número dos, se profundiza la investigación a través del marco teórico y las definiciones fundamentales de terminología básica que sustentan el presente trabajo de investigación, además se plantea los estándares utilizados en el desarrollo de los DRP's y el criterio de selección del estándar que se acople a nuestro trabajo de investigación.

En el capítulo número tres, se describe la situación actual de la Corporación AMCO, poniendo énfasis en la unidad de T.I. de AMCO, su infraestructura técnica, sus sistemas y aplicativos, así como los roles y responsabilidades del personal involucrado en el desarrollo del plan.

En el capítulo número cuatro entramos al desarrollo del Plan de Recuperación ante desastres basado en el estándar seleccionado.

En el capítulo número cinco se presenta el esquema de pruebas, el procedimiento para medidas correctivas, así como el plan de capacitación y concienciación.

Finalmente, en el capítulo número seis se detallan los inconvenientes encontrados y los resultados obtenidos tomando en cuenta los objetivos propuestos.

CAPÍTULO 1

GENERALIDADES

Hoy en día las compañías realizan sus operaciones diarias apoyándose en herramientas tecnológicas, las cuales deben de tener una alta disponibilidad al brindar sus servicios, por lo que deben ser capaces de manejar algún nivel de contingencia; sucesos como el acontecido el pasado 16 de abril de 2016, pondrían en riesgo la existencia de las mismas. Es aquí donde se origina la gestión de la continuidad del negocio conocido como BCP por sus siglas en inglés de Business Continuity Plan, que gracias a los diferentes planes que la conforman nos ayuda a minimizar los problemas que se van dando durante este tipo de sucesos y mejorando la respuesta del personal a cargo. Uno de esos planes que están dentro del BCP es el Plan de Recuperación ante desastres o DRP, el cual está dirigido al área de tecnología.

Dicha gestión tiene sus bases en el estándar británico 25999 y las normas ISO 27001 y 22301, que nos van a ayudar a elaborar el plan de recuperación ante desastres para poder contar con una serie de procedimientos a seguir direccionados a la mitigación del suceso. [1]

Actualmente ninguna compañía debería estar ajena a estas buenas prácticas, en virtud de que una caída en sus servicios degradaría su imagen tanto financiera como jurídica, llegando incluso a poner en riesgo su permanencia en el mercado.

1.1. Antecedentes

En virtud de los últimos eventos telúricos acontecidos en el país, los planes de recuperación ante desastres han tomado un suscitado protagonismo. La demanda de disponibilidad aumentó y se ha vuelto una necesidad en la mayoría de las compañías y del personal a cargo de las T.I., que se ven en la obligación de analizar si sus procesos pueden soportar un siniestro u otro tipo de calamidad, lo que nos demuestra que no solo debemos de cuidarnos de ataques informáticos sino además de cuidar el tiempo que los sistemas estén fuera de servicio, requisito fundamental en cada una de las actividades empresariales. Alcanzar una apropiada continuidad, expresa el acatamiento de estándares de buenas prácticas aplicables en el día a día y no esperar la ocurrencia de algún siniestro; eligiendo el más adecuado entre el estándar británico 25999 o una de las normas ISO internacionales.

Según el Horizont Scan Report del BSI [2], el 50% de las empresas a nivel de la región de América Central y Sur, utiliza la norma ISO 22301 en temas de continuidad; en lo que respecta a Manabí son escasas las compañías que implementan este tipo de normas ISO que les brinde

alta disponibilidad en sus operaciones ante sucesos inesperados, que les puedan ocasionar desde quebrantos económicos hasta cierres definitivos.

1.2. Descripción del problema

La Corporación AMCO, con sede en la ciudad de Manta, es un conjunto de compañías que brindan servicios integrales de agenciamiento, representación y abastecimiento a los armadores, operadores y otras empresas vinculadas al sector industrial, automotor, petrolero, naviero y pesquero en Ecuador y el mundo. Contribuye al desarrollo económico del país mediante el transporte y la comercialización de combustibles y líquidos vía marítima, además del transporte de contenedores vía terrestre por medio de vehículos tanqueros, cabezales y plataformas. Cuenta con sus respectivas áreas que conforman su personal administrativo altamente calificado y es capacitado de manera continua, para brindar el mejor de los servicios a la sociedad.

Actualmente la corporación cuenta con oficinas en Manta, Guayaquil y La Libertad, siendo la oficina principal en la ciudad de Manta, donde está alojado su Centro de Datos, que brinda todos los servicios tecnológicos a las diferentes empresas que conforman el grupo. Una eventualidad que ocurra en este CORE dejaría sin servicio a todas las empresas del Grupo por lo que es significativo disminuir el riesgo inherente.

En la oficina Matriz han tenido las siguientes afectaciones:

- La red de datos se vio comprometida por la propagación de un malware tipo troyano, afectando el rendimiento y productividad de sus usuarios.

- Caídas de servicio por hardware obsoleto en uno de sus equipos de Core.

En cuanto a inconvenientes fuera del Core tenemos:

- En múltiples ocasiones se han originado interrupciones del enlace de su proveedor entre las diferentes sucursales con Matriz, provocando la paralización de los servicios de los usuarios de sitios remotos.

En el año 2014, la Corporación AMCO fue objeto de una auditoría externa, evidenciando hallazgos y estableciendo observaciones y recomendaciones para el área de T.I., específicamente en temas de continuidad del negocio. Por este motivo es necesario realizar el Plan de Recuperación ante desastres para el departamento de tecnología de la Corporación, que le permita dar cumplimiento a estas recomendaciones.

1.3. Alcance

El motivo de implementación del DRP es la continuidad de las operaciones de los servicios brindados por la Unidad de TI de AMCO.

Debido a los diferentes sucesos ocurridos como la propagación de malware, las caídas de servicio por hardware obsoleto, las múltiples interrupciones con el enlace de su proveedor y además el informe expuesto en su última auditoría en el área de TI de la empresa, haciendo denotar la carencia del plan de recuperación ante desastres, se hace necesario crear un DRP para la unidad de TI de la empresa que pueda mitigar las posibles consecuencias que ocasionan estos acontecimientos.

1.4. Solución propuesta

Actualmente la tecnología se ha vuelto un recurso imprescindible en las labores diarias de toda empresa, ya sea grande o pequeña, lo que origina la necesidad de poseer un plan de recuperación antes desastres para el área de TI, que nos ayude a estar preparados ante cualquier suceso, sea este generado por la naturaleza o por el mismo hombre, estos eventos provocarían caídas en los servicios, perdidas y errores en la información, falsificación en los datos, etc., evidenciándose lo susceptible que somos a este tipo de eventos, a menos que se tengan implementadas las soluciones adecuadas.

Con el paso del tiempo la Corporación AMCO ha ido creciendo con ayuda de la tecnología, no obstante, al presentarse una contingencia no se cuenta con un plan donde se defina lo que debe realizar en un periodo de tiempo especificado. Por lo tanto, es obligación controlar estos desastres minimizando y administrando sus riesgos.

La Corporación AMCO busca el mejoramiento continuo de sus servicios, siendo el principal, la Comercialización de combustibles, esperando que estén siempre operativos manteniendo confianza y fidelidad de sus clientes.

Teniendo en cuenta la proyección de crecimiento de su cartera de clientes, así como su volumen de ventas y en vista de los hallazgos encontrados en su última auditoría; se propone la elaboración de un plan de recuperación ante desastres (DRP) al área de T.I., que permita mejorar su respuesta ante los posibles eventos, definiendo directrices a cumplir ante situaciones adversas. La ejecución del plan incrementará su nivel de respuesta ante estas eventualidades y así poder continuar con sus actividades diarias.

1.5. Objetivo General

Desarrollar un Plan de Recuperación ante desastres (DRP) para la unidad de T.I. de la Corporación AMCO seleccionando un estándar internacional conveniente, que ayude a mantener la continuidad del negocio ante posibles desastres.

1.6. Objetivos Específicos

- Definir y comprender los servicios, procesos y recursos críticos que estén inmersos en la unidad de T.I. de la corporación AMCO, y que cumplan con estándares internacionales para la creación del plan de recuperación ante desastres.
- Analizar estándares de continuidad acordes al negocio, tendencias actuales y realidad del entorno donde opera la compañía, para poder realizar un plan de recuperación ante desastres de T.I.
- Desarrollar el plan de recuperación ante desastres
- Diseñar pruebas pilotos para el plan de recuperación ante desastres.

1.7. Metodología

La metodología a seguir será: Se iniciará con reuniones de trabajo con los responsables de T.I. para definir temas claves como lo son el alcance del proyecto, el cronograma de trabajo, roles, comprender los servicios de la Corporación, procesos y recursos críticos que están inmersos en este departamento, para luego ser valorado con la Junta Directiva. Esto se lo realizará en diferentes reuniones con los responsables de cada servicio, para luego efectuar una comparación con los diferentes procesos si cumplen con algún lineamiento o norma

para realizar una tarea específica, caso contrario se planteará una sugerencia con una de las normas escogidas. Se diseñará un plan de recuperación ante desastres que será evaluado y probado por los directivos de la empresa. Una vez diseñada las pruebas piloto, se entregará este marco aprobado que sería el plan de recuperación ante desastres para la empresa, con los esquemas que pueden servir para cualquier eventualidad.

CAPÍTULO 2

MARCO TEÓRICO

2.1. Antecedentes (Preámbulo)

Un Plan de recuperación ante desastres o DRP (del Inglés Disaster Recovery Plan), ayuda y da soporte para que una organización restaure sus funciones en el área de tecnología de información y siga en funcionamiento después de un desastre. En este Plan se describen el marco y los procedimientos que deben seguirse en el caso que ocurra un desastre.

El DRP debe de abordar las siguientes áreas:

- **Prevención (antes del desastre):** “La organización debe primero asegurar los sistemas vulnerables, proteger los sistemas que contienen datos importantes y capacitar al equipo de la recuperación de desastres” [3]. Esta planificación hará que sea mucho más fácil y rápida para la recuperación.

- **Continuidad (Durante un desastre):** “En esta fase, el objetivo principal es mantener y continuar las operaciones críticas que permiten a la organización funcione correctamente” [4]. Incluye el mantenimiento de los sistemas y recursos críticos, así como su traslado a sitios secundarios durante un desastre.
- **Recuperación (después del desastre):** “Esta fase incluye la restauración de todos los sistemas y recursos a su estado normal y en pleno funcionamiento” [5]. Todos los sistemas y recursos presentes en ubicaciones secundarias son llevados de vuelta al sitio original.

2.2. Definiciones Fundamentales

Para la elaboración del presente trabajo, se han utilizado las siguientes definiciones:

Amenaza

“Persona, situación o evento natural del entorno (externo o interno) que es visto como una fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos.” [6]. Esta definición nos indica que todo evento, persona o situación ya sea externo o interno y que genere un riesgo para la institución es considerado una amenaza.

Incidente de Trabajo

“Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo” [7]. Resumiendo, un incidente de trabajo es todo suceso que causa o merma una paralización en las operaciones de un proceso.

Datos

“Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.” [8]. Son considerados datos todo tipo de registros, texto, imágenes, etc., que al ser estos procesados se convierten en información.

Disponibilidad

“La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, igual que los recursos necesarios para su uso.” [6]. La disponibilidad nos indica que tanto la información como los recursos deben estar siempre operativos para cuando se los necesita.

Integridad

“Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.” [8]. La integridad nos indica que los datos que fueron ingresados y procesados en el sistema se conserven igual y no sufran algún cambio en su contenido.

Desastre

“Un desastre es un evento calamitoso, repentino o previsible, que trastorna seriamente el funcionamiento de una comunidad o sociedad y causa unas pérdidas humanas, materiales, económicas o ambientales que desbordan la capacidad de la comunidad o sociedad afectada para hacer frente a la situación a través de sus propios recursos. Aunque frecuentemente están causados por la naturaleza, los desastres pueden deberse a la actividad humana.” [9]

Teniendo una definición de desastre desde el punto de vista de empresas sería como: “Un evento que hace que la continuación de los servicios y funcionalidades normales de la empresa, sean imposibles. Así, un DRP se compone de las precauciones a tomar para que los efectos de un desastre se reduzcan al mínimo y la organización sea capaz de mantener o reanudar rápidamente sus servicios y funcionalidades, al menos las de misión crítica.” [10]. Resumiendo, un desastre es todo evento inesperado o previsible que interrumpe con las operaciones normales de una organización.

Vulnerabilidad

Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Institución. Ejemplos: Deficiente control de accesos, poco control de versiones de software, entre otros. [6]. La vulnerabilidad es la explotación con o sin intención de la carencia de controles dentro de una institución.

Riesgo

Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la Entidad. [6]. Se define riesgo como la posibilidad de ejecución de una amenaza que cause un gran impacto en la institución.

Frecuencia

Estimación de ocurrencia de un evento en un período de tiempo determinado. Los factores a tener en cuenta para su estimación son la fuente de la amenaza y su capacidad y la naturaleza de la vulnerabilidad. [6]. Se define como frecuencia al número de repeticiones de un evento en un intervalo de tiempo.

Impacto

Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, reputación, disminución de capacidad de respuesta y competitividad, interrupción de las operaciones, consecuencias legales y afectación física a personas. Mide el nivel de degradación de uno de los siguientes elementos de continuidad: Confiabilidad, disponibilidad y recuperación. [6]. Se define como impacto a las consecuencias que provoca un hecho y que afectan a una institución.

Control

Cualquier actividad o acción realizada manual y/o automáticamente para prevenir o corregir irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos. [8]

Es el proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas. [6]. Se define como control a toda actividad que minimice la ocurrencia de un evento que afecte las operaciones normales de una institución.

Riesgo inherente

Es el cálculo del daño probable a un activo de encontrarse desprotegido, sin controles. [6]. Resumiendo, el riesgo inherente es intrínseco para cada actividad, sin tomar en cuenta los controles.

Riesgo residual

Riesgo remanente tras la aplicación de controles. [6]

Como nos indica en el riesgo residual la empresa asumirá su ocurrencia porque se aplicaron todos los controles posibles eficazmente pero no se puede erradicar del todo.

Sistema de Información

“Un sistema de información se puede definir técnicamente como un conjunto de componentes relacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control en una organización.” [11]

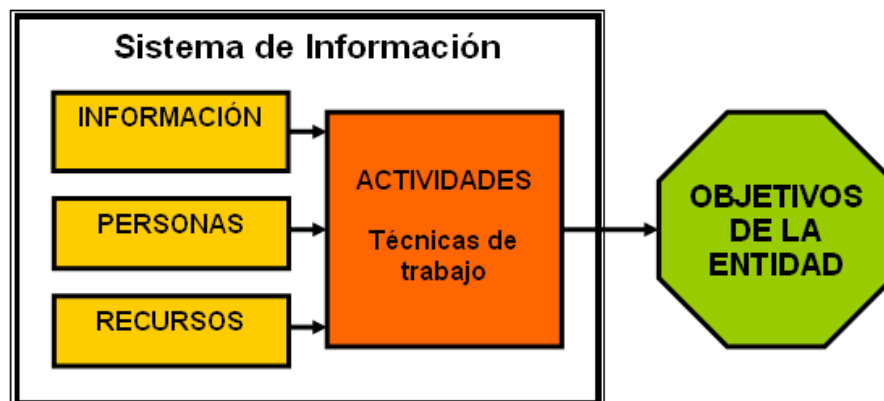


Figura 2.1: Sistema de Información

Todos los componentes están interrelacionados según su categoría en que se encuentren, las personas recolectan la información, esta información es tratada o procesada por un recurso informático mediante alguna técnica de trabajo que va a permitir que esa información ya procesada sea visualizada por las personas adecuadas.

Sistema Informático

Un sistema Informático “puede ser definido como un sistema de información que basa la parte fundamental de su procesamiento, en el empleo de la computación, como cualquier sistema, es un conjunto de funciones interrelacionadas, hardware, software y de Recurso Humano. Un sistema informático normal emplea un sistema que utiliza dispositivos que se usan para programar y almacenar programas y datos.” [12]

Otra definición dada en el Libro de Seguridad Informática es el que está “constituido por un conjunto de elementos físicos (hardware, dispositivos, periféricos y conexiones), lógicos (sistemas operativos, aplicaciones, protocolos,) y con frecuencia se incluyen también los

elementos humanos (expertos en el manejo de hardware y software)” [13]

Para resumir y enlazar con el concepto anterior de sistema de información, el sistema informático se trata de la parte de los recursos informáticos y las personas que usan esos recursos en el tratamiento de la información.

Gobierno de TI

Pablo Caneo Presidente de ISACA Capítulo Santiago de Chile explica Gobierno de TI “como una estructura de relaciones y procesos para dirigir y controlar la compañía hacia el logro de sus objetivos mediante la adición de valor, a la vez que mantiene un adecuado equilibrio entre riesgo y beneficio sobre TI y sus procesos”. [14]

Se trata que todos los procesos y mecanismos beneficien a la Empresa con la ayuda de TI; tratando con esto que se satisfagan las necesidades que tenga la institución, agregue valor en sus procesos, sean administrados adecuadamente y sobretodo que siempre los riesgos sean controlados.

Administración del Plan de Continuidad de Negocios

Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio. Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca las personas, procesos de negocios, tecnología e infraestructura. [6]

Este proceso administrativo busca que las actividades de la Empresa sean retomadas en el menor tiempo posible luego de la interrupción,

según su planificación, teniendo el compromiso de cada persona que trabaje en la empresa para que esto ocurra a la par con sus tareas designadas en estos sucesos inesperados.

Problema de Continuidad de Negocio

Es un evento interno o externo que interrumpe uno o más de los procesos de negocio. El tiempo de la interrupción determina que una situación sea un incidente o un desastre. [6]

Se debe de recalcar, en el caso que ocurra esta interrupción, es necesario verificar que actividades fueron afectadas y que se hace para que retome a sus actividades normales de funcionamiento. Es una parte del plan de continuidad

Análisis de Impacto del Negocio (BIA)

Es la etapa donde se analizan los riesgos presentes en el entorno, para determinar qué riesgos se pueden mitigar, cuáles se pueden transferir y cuáles se deben asumir. No es posible eliminar todos los riesgos, sino que se pueden mitigar (empleando medidas para reducirlos), transferir (ceder su responsabilidad a otra persona) o asumir (cuando se decide correr el riesgo con sus posibles consecuencias). Sin embargo, siempre existen riesgos remanentes y desconocidos. Es más, constantemente surgen nuevos riesgos a medida que la tecnología avanza y los sistemas cambian. Los entornos informatizados suelen acompañar estos cambios, adaptándose a los requerimientos tecnológicos del momento. [8]

Para resumir el BIA, identificará las funciones o procesos importantes de la empresa en caso de la interrupción por algún riesgo, revisará las consecuencias de lo acontecido y los tiempos de recuperación de

todas las operaciones interrumpidas según la prioridad. Sin embargo, siempre quedarán riesgos residuales y aparecerán nuevos riesgos, haciendo que sea conveniente actualizar este documento si llegara a suceder una nueva eventualidad que interrumpa con el funcionamiento normal de los procesos de la empresa.

Continuidad del Negocio

Una definición clara y precisa es la de SANS Institute como “las actividades requeridas para mantener a la organización en ejecución durante un período de desplazamiento o interrupción del funcionamiento normal.” [15]

Es parte del plan de recuperación, que aclara que se debe hacer en el caso de que ocurra la interrupción.

Recuperación de desastres

“La recuperación de desastres es el proceso de reconstrucción de su infraestructura de operación o después que el desastre haya pasado” [15]

En este caso este proceso es posterior al desastre y trata de reconstruir todas las operaciones afectadas.

Plan de contingencia

“Un Plan de contingencia se lo define como el conjunto de tareas que una organización define para enfrentar una crisis ya sea de tipo organizativa como de tipo tecnológica, para evitar la interrupción parcial o total de los servicios u operaciones. Para establecer las estrategias se realiza un proceso de análisis y se deben definir metodologías para determinar los procesos críticos.” [16]

Plan de continuidad del Negocio BCP (Business Continuity Plan)

“Es un conjunto de procedimientos y la información que se desarrolla, recolecta y mantiene preparado para su uso en caso de una emergencia o desastre " [15]

Si bien es cierto el concepto de BCP viene siendo algo breve, en el apartado 2.3 se hablará más de él dando diferencias fundamentales entre el BCP y DRP.

2.3. Plan de Recuperación ante Desastres (DRP)

“Es un proceso documentado o conjunto de procedimientos para recuperar y proteger la infraestructura tecnológica de una empresa en caso de un desastre [17]”.

Considérese como desastre, a la afectación de los datos, hardware o software, de forma natural, premeditada o inconsciente, que afecta a la continuidad de las operaciones de la compañía.

El plan de recuperación ante desastres se lo incluye dentro de un conjunto de planes conocido como Plan de Continuidad de Negocios o Business Continuity Plan (BCP), este último conformado por los siguientes componentes:

- Plan de reanudación de negocios.
- Plan de emergencia del personal.
- Plan de continuidad de operaciones.
- Plan de manejo de incidentes.
- Plan de recuperación de desastres.

Una de sus principales diferencias entre DRP y BCP es el alcance. El DRP está limitado a los procesos de TI, y este a su vez forma parte del BCP, compuesto principalmente por los procesos críticos del negocio, incluido el Plan de recuperación de desastres.

Por lo tanto, “la recuperación ante desastres se enfoca en el restablecimiento de los sistemas e infraestructura de TI que soportan los procesos de negocio críticos después de eventos de interrupción, mientras que la continuidad del negocio está orientada a la recuperación de los procesos de negocio críticos que son necesarios para la operación, por lo que no solo incluye lo anterior, sino también todos los demás aspectos operativos necesarios dentro de la organización [18]”.

Para el desarrollo y activación del DRP se deben tomar en cuenta los siguientes pasos:

- 1. Desarrollar la política de continuidad del negocio.** La continuidad del negocio tiene que estar presente en todas las operaciones de la compañía, por lo que debe de existir una política que establezca el marco de trabajo del plan para tener en cuenta los procesos críticos del negocio.
- 2. Realizar la evaluación de riesgos.** Nos permite la identificación, el análisis y la evaluación de los riesgos que afectarían al negocio.
- 3. Realizar el análisis de impacto del negocio.** Se definen el periodo de tiempo de recuperación de una función del negocio (RTO), y la antigüedad máxima de la información para su recuperación (RPO).

- 4. Desarrollar las estrategias de recuperación y continuidad del negocio.** Desarrollar y poner en práctica las medidas necesarias para volver a operar lo más pronto posible, tomando en cuenta las consideraciones de los puntos anteriores.
- 5. Concientizar, capacitar y probar el plan.** Una vez desarrollado el plan es necesaria su difusión, principalmente entre los encargados de su ejecución. Además, son necesarias las pruebas tanto de verificación como completas.
- 6. Mantener y mejorar el plan.** Después de las pruebas se deben de realizar mejoras para disponer del plan actualizado y direccionado con los objetivos del negocio.

2.4. Estándares y Normativas utilizados en los DRP's.

Las diferentes normas y estándares utilizados por las compañías alrededor del mundo, tienen sus orígenes en la necesidad de poder manejar los riesgos y políticas para la seguridad, con la finalidad de mantener la continuidad de sus operaciones, todo esto gracias a la selección de un estándar que vaya de la mano con sus necesidades.

Actualmente la probabilidad de sufrir una eventualidad ha aumentado, por lo que las organizaciones han ido implementando normas de buenas prácticas que les ayuden a mitigar los riesgos ante los cuales están expuestos. Por lo que se plantea la ejecución de un DRP que defina los procesos críticos dentro del departamento de T.I. A continuación, revisaremos los principales estándares para aseguramiento de la continuidad:

BS 25999

“La primera norma británica del mundo para la gestión de continuidad de la actividad comercial (BCM), se ha concebido para ayudar a minimizar el riesgo de interrupciones de estas características”. [19]

La norma fue publicada en dos partes:

BS 25999-1:2006 Parte 1: Documento de orientación que suministra el código de práctica del BCM.

BS 25999-2:2007 Parte 2: Se establecen las especificaciones para el BCM, y brinda la posibilidad de certificación para quienes cumplan los requisitos de la norma.

Los elementos que conforman cada parte son:

BS 25999-1:2006 – Código de práctica

- Gestión de Continuidad del Negocio.
- Política de Gestión de Continuidad del Negocio.
- Gestión del Programa de Continuidad del Negocio.
- Entendiendo la Organización.
- Desarrollo e Implementación de Respuestas a BCM.
- Determinando estrategias de Continuidad del Negocio.
- Ejercitando, Manteniendo y Analizando el plan de BCM.
- Fijando el BCM en la Cultura de la Organización.

BS 25999-2:2007 – Especificación

- Planeación del Sistema de Gestión de BCM.
- Implementando y Operando el Sistema.
- Monitoreo y Revisión del Sistema.
- Mantenimiento y Mejora del Sistema.

Clausulas.

Alcance.

Identificamos los procesos core del negocio que van hacer parte de la continuidad. Se escogerán los procesos de mayor importancia y en la que se basa su operación, prescindiendo de aquellos que se ejecuten en menor frecuencia. Existe la opción de incluirlos todos, decisión que tomará la corporación durante la ejecución de la normativa.

Términos y definiciones.

Terminología propia de la norma que se debe tener en cuenta.

Planear el BCMS.

Contiene la definición de políticas e incluye además la asignación de los recursos durante la ejecución de los BCMS. Además de la preparación de la documentación del sistema que incluya sus políticas y procedimientos.

Implementar y operar el BCMS.

Se necesita tener un mayor conocimiento de la corporación, lo que nos ayudará al desarrollo del sistema de continuidad, forma parte el BIA (Business Impact Analysis), el cual incluye las actividades críticas, el

impacto generado por la interrupción de estas actividades, definir el tiempo máximo tolerable de paralización, la dependencia entre ellas, identificar acuerdos con quien nos brinda servicio, así como el establecimiento de tiempo de recuperación para estas actividades.

Lo siguiente es el análisis de riesgo que nos ayuda a la identificación de las amenazas y vulnerabilidades en los procesos críticos de la corporación, para luego definir cómo serán tratados estos riesgos.

Se debe de revisar y evaluar periódicamente esta información a través de la autoevaluación y los diferentes exámenes de auditoría.

Monitorear y revisar el BCMS.

Se establecen como actividades principales las auditorías internas y la revisión a través de la junta directiva.

Mantener y mejorar el BCMS.

Fomentar la mejora continua de todo el sistema de continuidad gracias a las gestiones preventivas y correctivas.

ISO 22301:2012 – Sistemas de gestión de la continuidad de negocio

Es una norma creada por la ISO (Organización Internacional de Estandarización) especifica requerimientos para establecer y administrar efectivamente un Sistema de Gestión de Continuidad del Negocio (SGCN). [20]

ISO 22301 es la nueva norma internacional de gestión de continuidad de negocio que, a través del ciclo de mejora continua (PDCA), establece los requisitos para la planificación, el establecimiento, la

implantación, la operación, la supervisión, la revisión, la prueba, el mantenimiento y la mejora de un SGCN documentado, teniendo en cuenta la gestión de los riesgos globales de cada organización. [21]

En la misma página web de [21] expresa: “Una adecuada gestión de la continuidad del negocio permite a las organizaciones:

- Tener la capacidad de resistir los efectos de un incidente (resiliencia) así como prevenir o evitar los posibles escenarios originados por una situación de crisis.
- Gestionar la interrupción de sus actividades minimizando las consecuencias económicas, de imagen o de responsabilidad civil derivadas de la misma.
- Adquirir una mayor flexibilidad ante la interrupción de sus actividades.
- Reducir los costes asociados a la interrupción.
- Evitar penalizaciones por incumplimiento de contratos como proveedor de productos o servicios.
- Disponer de una metodología estructurada para reanudar sus actividades después de una interrupción.
- Aumentar su prestigio ante clientes y partes interesadas.
- Posibilidad de ventajas económicas a la hora de contratar seguros empresariales.”

Por medio de este estándar se enfatiza la importancia para entender la continuidad y necesidades de prepararse ante interrupciones,

estableciendo políticas de gestión de continuidad y objetivos. Para el cumplimiento de estas políticas, se implementan y operan controles y medidas para la gestión global de los riesgos de continuidad, que serán monitoreados para revisar el desempeño y efectividad y de acuerdo a estas mediciones hacer una mejora continua.

Proporciona una base para entender, planificar, desarrollar, implantar, monitorear, revisar, mantener y mejorar continuamente un SGCN documentado y con este poder responder oportunamente y recuperarse cuando suceda algún tipo de interrupciones, de esta forma se brinda confianza a nivel de negocios. En el SGCN como todo sistema de gestión se compone de:

- Política general del sistema
- Personas encargadas con responsabilidades definidas
- Gestiones de políticas, planeación, implementación y operación, evaluación de desempeño, revisiones y mejoramiento
- Documentación que pueda servir de evidencia para una futura auditoria
- Procesos de gestión relevantes de la organización que se pueda tomar en cuenta

Todos los requisitos que son especificados en la ISO 22301 son genéricos para poder ser aplicados a cualquier empresa u organización sin importar el tipo, tamaño y naturaleza, y su aplicación depende del ambiente operativo y de la complejidad de los procesos en la organización.

Como se dijo, este estándar aplica el ciclo de mejora continua PDCA (Por sus siglas en inglés de: Plan – Do -Check – Act), asegurando de esta manera un grado de compatibilidad con otros estándares como el ISO 9001, 14001 y otras que puedan ser aplicadas en cualquier momento por la empresa.

Con este estándar se trata agregar:

- Una mayor importancia en establecer objetivos para la empresa, así como el uso de indicadores para mejorar el desempeño.
- Mejor expectativa de parte de la alta dirección de la empresa.
- Asegurar una adecuada administración de recursos para que puedan ser provisionados en caso de escases o desastres y permita la continuidad.

A continuación, se describirán brevemente las cláusulas de esta norma:

Cláusula 1.- Alcance: Especifica los requisitos para planear, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado que pueda reducir las probabilidades de ocurrencia, estar preparados si estos ocurren, responder adecuadamente y recuperarse en el caso de incidentes que puedan surgir. [20]

Los requisitos especificados son genéricos para ser implementados en cualquier organización. Con esta norma se pretende que sea apropiada para las necesidades y requisitos de las partes interesadas de la organización como requerimientos regulatorios, organizacionales y de productos y servicios, entre otros.

Cláusula 2.- Referencias Normativas: Se basa en el documento en sí, que es indispensable. Para las referencias sin fecha se aplica la última edición del documento referenciado (incluye cualquier modificación); para las referencias fichadas se aplica únicamente la edición citada. [20]

Cláusula 3.- Términos y Definiciones: En este apartado se describen los términos y definiciones generales que se aplican en la norma ISO 22301, como las actividades, los procedimientos documentados que guían a la organización a responder, recuperar, reanudar y restablecer predefinidos después de una alteración, entre otros documentos para que implementar y mantener la continuidad del negocio. [20]

Cláusula 4.- Contexto de la organización: Indica que la organización deberá determinar los aspectos internos y externos que pueden afectar en la obtención de los resultados esperados en el SGCN, entender las necesidades y expectativas de las partes interesadas que intervienen y las normativas legales y reglamentarias aplicables. También se debe determinar el alcance y cuando será aplicado el SGCN. [20]

Cláusula 5.- Liderazgo: Hace referencia a las personas en la alta gerencia o en otros roles gerenciales en la organización, y su liderazgo y compromiso que deben demostrar con respecto al SGCN. Además, tiene que asegurar de proporcionar los recursos necesarios, establecer políticas y asignar responsabilidades a las personas que implementan y mantienen un SGCN y que son debidamente comunicadas dentro de la organización [20]

Cláusula 6.- Planeación: En esta sección se requiere identificar los riesgos para la implementación del sistema de gestión y establecer objetivos y criterios para medir el éxito. Así mismo la organización debe tener una información documentada de estos objetivos que se desean alcanzar y así determinar: los responsables, qué se hará y cuando se completará, que recursos serán necesarios, y cómo los resultados serán evaluados. [20]

Cláusula 7.- Soporte: Cláusula para que la organización debe determinar y proveer los recursos necesarios para todo el desarrollo y mejora continua del SGCN. Da una gran importancia a la competencia para el éxito de la continuidad del negocio, las que deben contar con conocimientos, habilidades y experiencia, para que puedan contribuir con el SGCN y responder efectivamente cuando algún incidente se produzca.

Devuelve la importancia a la toma de conciencia de las personas que trabajan en la organización con los temas de la política de gestión de continuidad, los beneficios de la mejora de desempeño por su contribución en el SGCN.

Además, se determina la necesidad para las comunicaciones relevantes al SGCN, tanto internas como externas, en el contexto de qué, cuándo y con quién se comunican, con una estructura con autoridades apropiadas y en capacidades durante los eventos que alteren las comunicaciones normales. Por último, también se habla de la información documentada que se mantenga actualizada, y cuando sea accedida por las personas adecuadas con los permisos pertinentes. [20]

Cláusula 8.- Operación: La organización debe establecer, implementar y mantener un proceso documentado y formal necesario de análisis del impacto del negocio y evaluación del riesgo para acciones a tomar en caso de interrupciones.

Se establecerá criterios de evaluación, tomar requerimientos legales y otros en los que la empresa esté suscrita, analizar los controles de riesgo, tratamiento y costos relacionados. Luego de analizar el impacto que apoyan la provisión de productos y servicios, el tiempo de reanudar actividades a un nivel aceptable, e identificar las dependencias y recursos de apoyo de estas actividades, incluyendo suplidores, compañeros de outsourcing y partes interesadas relevantes.

Se debe evaluar los riesgos de una interrupción priorizando con los que requieren tratamiento y recuperación más inmediata y por último establecer la estrategia que le permita a niveles aceptables la continuidad de operaciones del negocio. [20]

Cláusula 9.- Evaluación del desempeño: Se trata medir y evaluar todo tipo de acción o correctivo tomado en la organización, monitorear procesos, estado de problemas internos y externos, realizar auditorías internas y externas y revisar sus estados; tener en cuenta oportunidades de mejorar continuamente, si se necesitan cambios, cuando se observaren no conformidades, también las opiniones de proveedores y socios y cualquier cambio que pudiera afectar el SGCN. Estas revisiones deben ser revisada por la alta dirección a intervalos planificados, para asegurar su continua adecuación, conveniencia y efectividad. [20]

Cláusula 10.- Mejora: Se debe de identificar la no conformidad, reaccionar ante ellas, tomar acciones para controlarla, y corregirla, además de tratar sus consecuencias. También se debe evaluar las acciones para eliminar las causas para que no haya ocurrencia en el mismo lugar u otro, revisando su efectividad sin olvidar de registrar los resultados de estas acciones correctivas, registrando los cambios al SGCN cuando fuera necesario. La organización puede utilizar los procesos de: liderazgo, planeación, y evaluación del desempeño para alcanzar la mejora. [20]

ISO 27001

“Esta norma internacional ha sido elaborada con la finalidad de proporcionar los requisitos para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información (SGSI).

El SGSI conserva la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión del riesgo y garantiza, a las partes interesadas, que los riesgos sean manejados adecuadamente.” [22]

Cláusulas de la ISO 27001 [22]:

1. Introducción
2. Alcance.
3. Referencias Normativas.
4. Términos y definiciones.
5. Contexto de la Organización.

6. Liderazgo.
7. Planificación.
8. Apoyo / Soporte
9. Operación
10. Evaluación del desempeño
11. Mejora.

2.5. Modelo PDCA.

Es un esquema utilizado por las normas ISO 22301 e ISO 27001, que soporta las operaciones y la continuidad de los servicios de T.I.

Está basado en el ciclo de Deming Plan-Do-Check-Act (del inglés PDCA). En virtud de tener siempre los servicios operativos, se toma en cuenta la aplicación de este modelo de gestión para soportar la operación de todos los procesos de tecnología que requiera el negocio en sus actividades diarias.

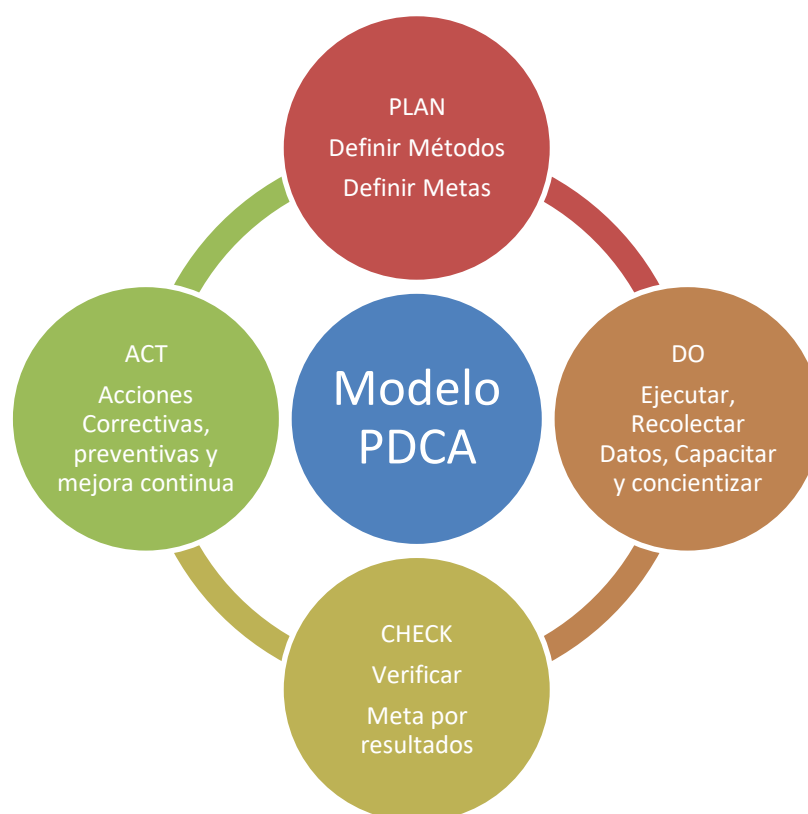


Figura 2.2: Modelo PDCA

Este modelo se basa en un análisis de impacto en el negocio, enfocándose en los procesos críticos soportados por los servicios de T.I. A continuación, se detallan las diferentes etapas con su documentación necesaria.

2.5.1. Fase de Planificación (PLAN).

Definición de objetivos y procesos necesarios para alcanzar los resultados requeridos por la organización, recopilando datos que nos ayuden en la comprensión de estos procesos. Los documentos necesarios son:

Tabla 1: Documentos de la Fase de Planificación

No.	Nombre del documento
1	Procedimiento para identificación de requisitos.
2	Lista de requisitos legales, normativos y contractuales.
3	Política para la recuperación ante desastres.
4	Plan de capacitación y concienciación.

2.5.2. Fase de Realización (DO).

Implementación de los nuevos procesos, se recomienda realizarlos a través de pruebas piloto para ir verificando su correcto funcionamiento antes de su aplicación final. Los documentos necesarios son:

Tabla 2: Documentos de la Fase de Realización

No.	Nombre del documento
1	Metodología para el análisis del impacto en el negocio.
2	Cuestionario sobre el análisis del impacto en el negocio.
3	Estrategia de recuperación ante desastres.
4	Lista de Actividades.
5	Prioridades de recuperación para las actividades.
6	Objetivos de tiempo de recuperación para las actividades.
7	Ejemplos de escenarios de incidentes disruptivos.
8	Plan de preparación para la continuidad de los servicios de T.I.
9	Estrategia de recuperación de actividad.
10	Plan de recuperación ante desastres.
11	Plan de respuesta a los incidentes.
12	Registro de incidentes.
13	Ubicaciones para la continuidad de las operaciones.
14	Plan de transporte.
15	Contactos claves.
16	Plan de recuperación de actividad.

2.5.3. Fase de Verificación (Check).

Durante un tiempo de prueba establecido, se verifica el correcto funcionamiento de la mejora implantada. Si los resultados no

son los esperados, se realizan cambios para conseguir los objetivos deseados. Los documentos necesarios son:

Tabla 3: Fase de Verificación

No.	Nombre del documento
1	Plan de prueba, mantenimiento y revisión del DRP.
2	Informe de pruebas y verificación.
3	Plan de mantenimiento y revisión del DRP.
4	Formulario de revisión postincidente.
5	Procedimiento para auditoría interna.
6	Programa anual de auditoría interna.
7	Informe de auditoría interna.
8	Lista de apoyo auditoría interna.
9	Minutas de revisión por parte de la dirección.

2.5.4. Fase de Ajuste (ACT).

Aplicación de mejoras cuando se detectan errores durante la ejecución de una iteración del modelo. Los documentos necesarios son:

Tabla 4: Fase de Ajuste

No.	Nombre del documento
1	Procedimiento para medidas correctivas.
2	Formulario para medidas correctivas.

2.6. Selección del estándar a aplicar

Para la selección del estándar se escogieron criterios que se ajusten al entorno del departamento de T.I. de la Corporación AMCO, de esta forma alcanzar unos resultados más precisos y que mitiguen de una mejor manera los riesgos.

Entre los criterios de selección tenemos:

- Aporte a la continuidad: Aseguramiento de la continuidad en temas tecnológicos y operativos del negocio.

- Capacidad de ajuste: La facilidad para adaptarse a los cambios según las necesidades de cada organización.
- Alcance global: El grado de aplicación y presencia internacional que tiene el estándar.
- Mejora continua: Actualización periódica de la norma respaldada por una entidad internacional que se preocupe por mejorar de forma continua el estándar.
- Adaptabilidad: La aplicación de la norma no afecte a los procesos Core del negocio, y sea independiente del tamaño de la misma.
- Autonomía: No sea necesaria la aplicación previa de una norma para su puesta en marcha.
- Repercusión: El impacto que puede llegar a tener el estándar en la organización una vez implementado.
- Sostenible en el tiempo: La aplicación de la norma debe asegurar que sea exitosa y subsista en el tiempo.
- Calidad certificada: Una vez aplicada la norma, esta debe poder ser certificable, dando la seguridad que se cumplen con patrones de calidad.
- Casos de éxito: La experiencia es fundamental en la implementación de la norma, lo que nos ayuda a identificar errores y mejorar la utilización de los recursos.

Selección.

Se procede agrupar los criterios en una tabla para posterior calificar basándonos con un juicio personal una vez analizados los estándares declarados.

A continuación, se enlistan los 10 criterios que equivalen al 100% del estándar a emplear, se divide el 100% para la cantidad de criterios de selección, lo que se obtiene un total de 10% por cada criterio, por último, se califica cada norma tomando como referencia cada criterio de selección.

Tabla 5: Selección del estándar según criterios de selección

Ponderación	Criterio de Selección	Estándares		
		BS 25999	ISO 22301	ISO 27001
10%	Aporte a la continuidad.	100%	100%	35%
10%	Capacidad de ajuste.	100%	100%	80%
10%	Alcance global.	40%	100%	100%
10%	Mejora continua.	70%	90%	80%
10%	Adaptabilidad.	70%	90%	80%
10%	Autonomía.	90%	95%	80%
10%	Repercusión.	85%	85%	85%
10%	Sostenible en el tiempo.	60%	100%	90%
10%	Calidad certificada.	100%	100%	100%
10%	Casos de éxito.	80%	90%	90%
100%	TOTAL	79,5%	95%	82%

Una vez asignado los pesos y realizados los cálculos, se selecciona la norma ISO 22301, la que cuenta con la calificación más alta según los criterios examinados.

CAPÍTULO 3

DEFINICIÓN DE LA SITUACIÓN ACTUAL

3.1 Descripción del Departamento de T.I.

La Unidad de T.I de AMCO tiene como propósito mantener funcionales los sistemas informáticos e incorporar nuevas soluciones para la optimización de los procesos de la empresa.

3.2 Organigramas de la empresa y de T.I.

Estructura orgánica de AMCO

La Estructura Orgánica funcional de AMCO se encuentra desarrollada en forma lineal como se puede apreciar en la figura a continuación, orientada de arriba hacia abajo estando las principales autoridades sobre los niveles más altos:

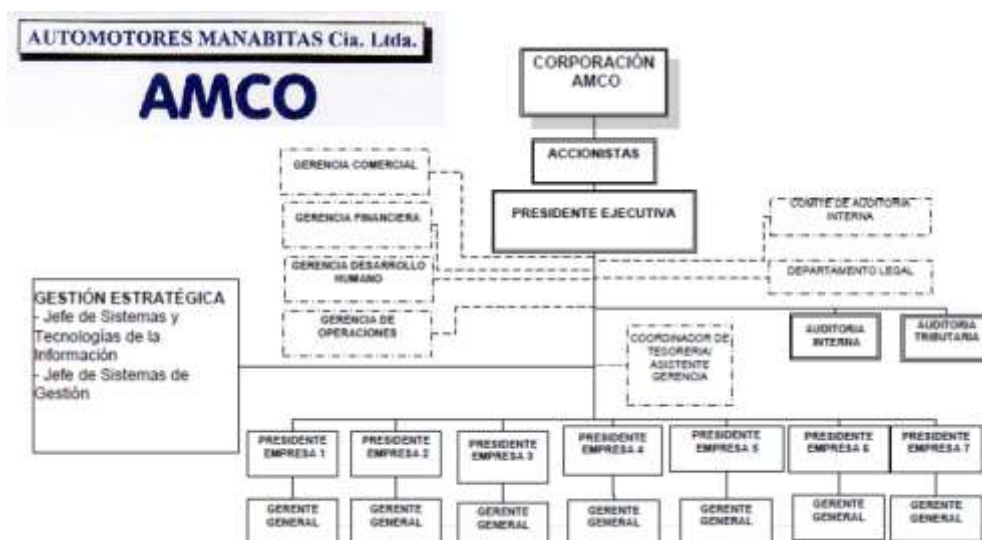


Figura 3.1: Estructura orgánica de AMCO

Misión y Visión de AMCO

Misión: Corporación AMCO comercializa productos derivados del petróleo y brinda soluciones logísticas, prestando unos servicios de manera ágil, oportuna y eficiente a sus clientes del sector marítimo e industrial, capitalizando su talento humano y generando rentabilidad a sus accionistas.

Visión: En el 2020, Corporación AMCO liderará la comercialización de productos derivados del petróleo y servicios logísticos integrales en el mercado ecuatoriano, siendo reconocida por sus clientes por un servicio de alta calidad a través del trabajo en equipo, mejora continua e innovación.

Estructura orgánica de la Unidad de TI.

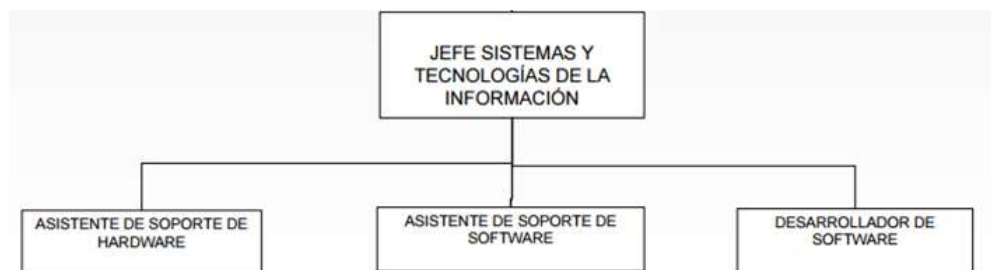


Figura 3.2: Estructura Orgánica de TI

SITUACIÓN ACTUAL DE AMCO.

Debido a que este tema se ha dirigido solamente para la Unidad de TI, se describirá la situación actual del departamento de TI

SITUACIÓN ACTUAL DEL DEPARTAMENTO DE TI DE AMCO

La unidad de TI es el departamento que tiene como propósito mantener funcionales los sistemas informáticos e incorporar nuevas soluciones para la optimización de los procesos de la empresa.

La unidad de TI de AMCO, es gestionada por el Jefe de Sistemas, Ing. Fernando Lectong. Las oficinas principales se encuentran ubicadas en la ciudad de Manta, la unidad de TI ubicada en Matriz gestiona el soporte vía remota a las sucursales de La Libertad y Guayaquil.

En la oficina Matriz han tenido las siguientes afectaciones:

- La red de datos estuvo comprometida por la propagación de un malware tipo troyano, afectando el rendimiento y productividad de sus usuarios.

- Caídas de servicio por hardware obsoleto en uno de sus equipos de Core.

En cuanto a inconvenientes fuera del Core tenemos:

- En múltiples ocasiones se han originado interrupciones del enlace de su proveedor entre las diferentes sucursales con Matriz, provocando la paralización de los servicios de los usuarios de sitios remotos.

En el año 2014, la Corporación AMCO fue objeto de una auditoría externa, evidenciando hallazgos y estableciendo observaciones y recomendaciones para el área de T.I., específicamente en temas de continuidad del negocio.

El 16 de abril de 2016, la provincia de Manabí se vio afectada por un fuerte terremoto provocando la paralización de las actividades comerciales en un sin número de empresas de la provincia. AMCO no fue la excepción y tuvo que improvisar un plan de acción posterior al evento sísmico para poder continuar con sus actividades, trabajando en un sitio alterno improvisado, evaluando los daños y el costo de las reparaciones del edificio matriz para la reactivación de sus actividades normales que duró aproximadamente 3 meses.

En virtud a lo sucedido, es necesario el desarrollo del Plan de Recuperación ante desastres para la unidad de T.I. de AMCO, que le permita sobrellevar de mejor manera las situaciones adversas y mejorar sus tiempos de recuperación.

La unidad de TI de AMCO, se divide en tres secciones para el cumplimiento de sus actividades:

Soporte de Hardware, Soporte de Software y Desarrollo de Software

Soporte de Hardware: Se encarga de brindar soporte a los usuarios y mantenimiento de los equipos y comunicaciones. Debido a su cartera de clientes internacionales, sus servicios necesitan que estén 24 horas al día, los 7 días a la semana, lo que obliga a tener personal altamente capacitado.

AMCO cuenta con 254 empleados en matriz y sus dos sucursales, dispone de 20 servidores que dan servicio a todos sus empleados y proveen la infraestructura a los diferentes sistemas con lo que cuenta la empresa. La persona encargada de esta sección administra lo siguiente:

- Computadores de escritorio
- Telecomunicación
- Gestión de Servidores y Aplicaciones
- Gestión de Usuarios

Cuenta con 118 computadores aproximadamente, de los cuales 67 son equipos portátiles y 51 de escritorio.

Con respecto a la gestión del nombre para los equipos de cómputo es la siguiente: Los 3 primeros caracteres son abreviatura del Departamento, las 3 siguientes abreviaturas pertenecen al puesto que ocupa el usuario, y los 2 últimos dígitos son una secuencia de números según corresponda.

En lo que respecta a la conectividad, sus equipos de telecomunicaciones (routers y switches) se encuentran en el edificio

matriz en Manta; desde donde se tiene conexión a las otras dos sucursales de Guayaquil y La Libertad. El enlace principal a internet es brindado por Telefónica Movistar y su secundario a través de Telconet. El mapa de red se detalla en el apartado 3.4 Infraestructura Técnica.

Soporte de software: Se encarga de dar soporte a los usuarios y mantenimiento a los programas, enlace y configuraciones. La persona encargada de esta sección, tiene como responsabilidad de gestionar las siguientes aplicaciones:

- EPR (Empresa por Resultados)
- Dynamics AX 2009
- Flexline
- Denwa

Desarrollo de Software: Se encarga de crear, modificar y mantener las aplicaciones de software de la empresa. El sistema contable Dynamics AX 2009, es uno de los principales dentro de la corporación. Utiliza como motor de base de datos SQL Server que permite manejar información de clientes, ventas, facturación, proveedores, pedidos, inventarios, etc. Físicamente se encuentra en la Ciudad Manta, en el Edificio Matriz y es accedido desde las sucursales de forma remota.

MAPEO DE SERVICIOS QUE SOPORTA LA UNIDAD DE TI A LOS DEPARTAMENTOS DE AMCO

Se enlistan por departamentos los servicios de TI que son demandados:

Tabla 6: Servicios de TI por Departamento

DEPARTAMENTO	SERVICIO DE TI
Finanzas	Dynamics AX Microsoft Office: Word, Excel, PowerPoint, Outlook FRX Qlikview Email Zimbra Firewall – Antispam - Sophos UTM Telefonía IP Denwa Backup Synology
Recursos Humanos	Flexline Saicom Sirha Microsoft Office: Word, Excel, PowerPoint, Outlook Email Zimbra Firewall – Antispam - Sophos UTM Telefonía IP Denwa Backup Synology
Comercial	Microsoft Office: Word, Excel, PowerPoint, Outlook Qlikview MobilVendor Email Zimbra Firewall – Antispam - Sophos UTM Telefonía IP Denwa Backup Synology
Operaciones	Microsoft Office: Word, Excel, PowerPoint, Outlook Saicom Email Zimbra Firewall – Antispam - Sophos UTM Telefonía IP Denwa Backup Synology
Sistemas	Microsoft Office: Word, Excel, PowerPoint, Outlook Email Zimbra Firewall – Antispam - Sophos UTM Telefonía IP Denwa Backup Synology

LISTADO DE PROCESOS DEL DEPARTAMENTO DE TI

Los principales procesos que desarrolla el departamento de TI son:

Tabla 7: Listado de los servicios de TI y su frecuencia de uso

PROCESOS DE TI	DESCRIPCIÓN	FRECUENCIA DE USO
Creación de Usuarios	Se crea usuario bajo petición del departamento de Talento Humano o Jefes departamentales.	Por petición de ingresos de personal
Obtención de backups	<ol style="list-style-type: none"> 1) Bases de datos 2) Información de usuarios. 3) Configuraciones de equipos (Central IP, Firewalls) 	<ol style="list-style-type: none"> 1) Diarios, Semanal 2) Semanal 3) Diarios
Mantenimiento de comunicaciones	Se hace mensualmente revisión de sistemas de comunicación y otros equipos, pero sin periodicidad fija dentro del mes.	Mensual
Mantenimiento de Hardware	Se hace mantenimiento en base a un plan anual diseñado y establecido a inicios de año.	Semestral (UPS, Impresoras), Anual (Computadores)
Mantenimiento de Software	Se hace mantenimiento en base a un plan anual diseñado y establecido a inicios de año.	Anual
Adquisición de equipos	Se hace las adquisiciones en base a un plan diseñado y aprobado a inicios de año más equipos pedidos por requerimiento emergente.	Mensual
Adquisición de software	Se hace las adquisiciones en base a un plan diseñado y aprobado a inicios de año más equipos pedidos por requerimiento emergente.	Mensual
Soporte a	Se brinda soporte diario en	Diario

usuarios	todas las aplicaciones y equipos informáticos, en edificio principal de forma presencial y en sucursales de forma remota.	
Capacitación a Usuarios	Se brinda capacitación al personal en el manejo de equipos y aplicaciones.	Bajo petición del departamento interesado.
Administración de Base de datos	Se gestiona todos los procesos sobre las bases de datos de las aplicaciones existentes	Semanal
Mantenimiento y Soporte del EPR	Se administra todas las funcionalidades y procesos del EPR	Semanal
Administración Web	Se administra y mantiene el diseño y contenido de la página Web	Mensual

Análisis FODA del Departamento de TI

Fortalezas

- Los procedimientos realizados se ejecutan en base a la información técnica recopilada para el efecto.
- El personal está calificado para administrar tanto equipos como aplicaciones.
- Se desarrolla una planificación a inicios del año para realizar el proceso de renovación de la plataforma tecnológica.
- Cualquier problema suscitado en las sucursales es transmitido hacia la matriz para su solución.
- La relación del personal de TI con los otros departamentos es muy buena.

Oportunidades

- La Unidad de TI tiene gran participación en los proyectos de la Empresa.
- Se accede a nuevas tecnologías gracias a convenios con proveedores.
- Se acceden a capacitaciones de tecnología reciente para mejorar las respuestas de la Unidad de TI.

Debilidades

- Acceso remoto y no local de los sistemas desde las sucursales y buques.
- Carencia en capacitación al personal de TI, la mayor parte es por autoaprendizaje.
- Gestión de TI desde matriz hacia las otras sucursales.
- Falta de personal de TI en las sucursales.
- Desconocimiento del negocio por parte de la gestión de TI.
- Carencia de presupuesto para la infraestructura de TI.
- Falta de personal en el cumplimiento de los procesos de TI.

Amenazas

- Copia no autorizada de nuevo software – hardware por parte de la competencia.
- Problemas con proveedores en la entrega-recepción de materiales.
- Problemas políticos que afecten al negocio.

3.3. Servicios del departamento de T.I.

La Unidad de TI dentro de la jerarquía funcional está ubicada como un área de ayuda a las autoridades principales, así como también apoyando en aspectos tecnológicos en los diferentes departamentos de la Corporación.

Entre los principales servicios que brinda TI están:

- Soporte técnico a Usuario en Hardware y Software.
- Mantenimiento preventivo y correctivo.
- Administración de servidores.
- Administración de aplicaciones.
- Desarrollo de aplicaciones.
- Actualizaciones de sistemas.
- Soporte a sucursales.
- Control de Backups de información.
- Administración de telefonía IP.
- Administración de Acceso Biométrico.

3.4. Infraestructura Técnica.

La red de la Empresa está distribuida por un sistema de routers y switches por los departamentos, al igual se tiene un enlace VPN para las sucursales de Guayaquil y La Libertad

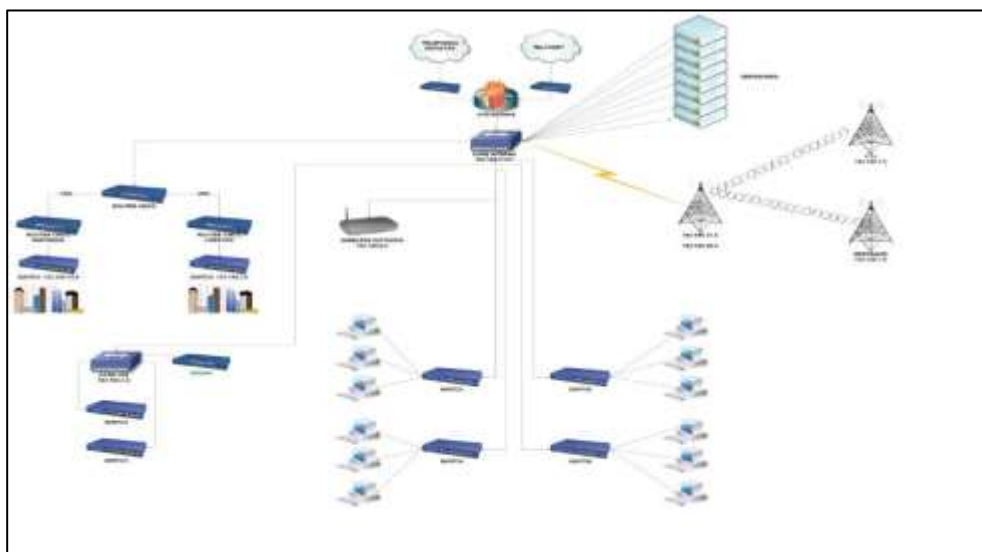


Figura 3.3: Infraestructura de red y dispositivos de AMCO

3.5. Aplicaciones

- EPR (Empresa por Resultados) – Sistema Planeación Estratégica. Con EPR, los factores estratégicos, humanos y operativos se enfocan a la planeación, ejecución y confirmación del desempeño organizacional. Su interfaz gráfica es web y muy agradable en cuanto a diseño. Funciona sobre un servidor Apache Tomcat y como servidor de base de datos utiliza Microsoft Sql Server.
- Dynamics AX 2009 – Sistema Contable. Microsoft Dynamics AX es uno de los productos de software de planificación de recursos empresariales (ERP) de Microsoft, perteneciente a la familia Microsoft Dynamics, este sistema nos permite manejar la información de nuestros clientes permitiendo realizar pedidos de ventas y manejar toda la facturación, también maneja proveedores, realizar pedidos de compra, crear artículos y manejo de inventarios, manejo de recursos, administración de proyectos entre otras infinidad de funciones, Dynamics AX es un ERP muy

complejo para el manejo de la información de medianas y grandes empresas. Se integra muy fácilmente con otras herramientas Microsoft como por ejemplo Microsoft Excel, para exportar información directamente desde AX, usa Base de Datos SQL Server y se instala sobre Microsoft Windows Server, para su utilización el sistema se ejecuta en casi cualquier versión de Windows.

- Flexline – Sistemas de Nomina. Administra todos los procesos de nómina. Funciona con una base de datos SQL Server con Windows Server.
- Denwa – Sistemas de telefonía IP. Nuevo concepto en comunicaciones empresariales que permiten un gerenciamiento integral de las comunicaciones de manera unificada. Es un servidor tipo Appliance sobre Linux que gestiona todas las comunicaciones Análogas o IP.

3.6. Implementación del modelo

La implementación de este modelo toma como base los diferentes sucesos ocurridos en la unidad de T.I. de AMCO y el desarrollo de este nuevo esquema sustentado en la norma ISO 22301, toda la documentación generada en el presente proyecto se encuentra detallada en los anexos.

Los anexos contienen los datos del modelo aplicado al presente proyecto, y pueden ser revisados en cada una de las fases del modelo PDCA, a continuación, se detalla la aplicación de cada una de estas fases.

3.6.1. Fase de Planificación (PLAN)

Definición de objetivos y procesos necesarios para alcanzar los resultados requeridos por la corporación AMCO, recopilando datos que nos ayuden en la comprensión de estos procesos. Los documentos relacionados con esta fase son:

Tabla 8: Fase de Planificación

No.	Nombre del documento	Anexo
1	Procedimiento para identificación de requisitos.	3
2	Lista de requisitos legales, normativos y contractuales.	3.1
3	Política para la recuperación ante desastres.	4
4	Plan de capacitación y concienciación.	9

3.6.2. Fase de Realización (DO)

Implementación en la corporación AMCO de los nuevos procesos, se recomienda realizarlos a través de pruebas piloto para ir verificando su correcto funcionamiento antes de su aplicación final. Los documentos necesarios se encuentran detallados en los siguientes anexos:

Tabla 9: Fase de Realización

No.	Nombre del documento	Anexos
1	Metodología para el análisis del impacto en el negocio.	5
2	Cuestionario sobre el análisis del impacto en el negocio.	5.1 5.2
3	Estrategia de recuperación ante desastres.	6
4	Lista de Actividades.	6.1

5	Prioridades de recuperación para las actividades.	6.2
6	Objetivos de tiempo de recuperación para las actividades.	6.3
7	Ejemplos de escenarios de incidentes disruptivos.	6.4
8	Plan de preparación para la continuidad de los servicios de T.I.	6.5
9	Estrategia de recuperación de actividad.	6.6 6.7
10	Plan de recuperación ante desastres.	7
11	Plan de respuesta a los incidentes.	7.1
12	Registro de incidentes.	7.2
13	Ubicaciones para la continuidad de las operaciones.	7.3
14	Plan de transporte.	7.4
15	Contactos claves.	7.5
16	Plan de recuperación de actividad.	7.6 7.7

3.6.3. Fase de Verificación (Check)

Durante un tiempo de prueba establecido, se verifica el correcto funcionamiento de la mejora implantada en la corporación AMCO. Si los resultados no son los esperados, se realizan cambios para conseguir los objetivos deseados. Los documentos necesarios se encuentran detallados en los siguientes anexos:

Tabla 10: Fase de Verificación

No.	Nombre del documento	Anexos
1	Plan de prueba, mantenimiento y revisión del DRP.	8
2	Informe de pruebas y verificación.	8.1
3	Plan de mantenimiento y revisión del DRP.	8.2
4	Formulario de revisión postincidente.	8.3
5	Procedimiento para auditoría interna.	10
6	Programa anual de auditoría interna.	10.1
7	Informe de auditoría interna.	10.2
8	Lista de apoyo auditoría interna.	10.3
9	Minutas de revisión por parte de la dirección.	11

3.6.4. Fase de Ajuste (ACT)

Aplicación de mejoras cuando se detectan errores durante la ejecución de una iteración del modelo en la corporación AMCO. Los documentos necesarios se encuentran detallados en los siguientes anexos:

Tabla 11: Fase de Ajuste

No.	Nombre del documento	Anexos
1	Procedimiento para medidas correctivas.	12
2	Formulario para medidas correctivas.	12.1

3.7. Roles y Responsabilidades

ASISTENTE DE SOPORTE DE HARDWARE

Funciones. - El asistente de Soporte de Hardware se encarga de dar soporte a los usuarios en Mantenimiento a los equipos y comunicaciones. Sus responsabilidades son:

- Instalar y mantener el software y hardware de la empresa, así como supervisar, actualizar y controlar su inventario.
- Dar soporte a usuarios en el uso de herramientas informáticas.
- Elaborar y ejecutar planes de mantenimiento preventivo de hardware y software.
- Administrar los sistemas antivirus de forma centralizada para el monitoreo de posibles contaminaciones.
- Reportar defectos en los equipos o suministros con los proveedores y realizar el seguimiento de las garantías correspondientes.
- Llevar una bitácora del soporte brindado.
- Programar, ejecutar y monitorear los sistemas de respaldo de información garantizando la disponibilidad de los mismos.
- Visita y soporte a los Sistemas y Equipos de buques y sucursales.

ASISTENTE DE SOPORTE DE SOFTWARE

Funciones. - El Asistente de Soporte de Software se encarga de dar soporte a los usuarios en Mantenimiento a los programas, enlaces y configuraciones. Sus responsabilidades son:

- Brindar soporte a los usuarios finales de las aplicaciones administrativas tales como: Ofimáticas, ERP, Sistema de mantenimiento de activos, Sistema de inteligencia de negocios, etc.

- Ejecutar pruebas de funcionalidades a nuevas aplicaciones para el mejoramiento de los procesos de la empresa.
- Realizar capacitaciones a los usuarios en el manejo de las aplicaciones.
- Realizar mantenimiento a las aplicaciones web de la empresa.
- Elaborar y ejecutar planes de mantenimiento preventivo de equipos de apoyo.
- Escalar el soporte al área de desarrollo en caso de requerirse mejoras o mantenimiento a los sistemas de información o realizar el respectivo reporte a los proveedores externos y realizar el seguimiento de las soluciones correspondientes.
- Administración de los usuarios de los diferentes sistemas y aplicaciones.
- Llevar una bitácora del soporte brindado.

DESARROLLADOR DE SOFTWARE

Funciones. - El desarrollador de software se encarga de crear, modificar y mantener aplicaciones de software. Sus Responsabilidades son:

- Coordinar y desarrollar los proyectos y procesos, mediante planes de trabajo que consideren las necesidades de información de las áreas solicitantes.

- Desarrollar aplicaciones, reportes y demás funcionalidades requeridas por los usuarios de la empresa.
- Participar en el establecimiento de estrategias y criterios metodológicos para el diseño y desarrollo de sistemas.
- Validar la funcionalidad de las aplicaciones, así como las soluciones viables a las necesidades informáticas de la empresa, mediante continua interacción con las áreas involucradas.
- Generar la documentación técnica y manuales de usuarios de las aplicaciones desarrolladas.
- Brindar asesoría y asistencia técnica permanente a los usuarios del área de soporte, sobre los sistemas implementados.
- Llevar un registro de los desarrollos realizados.

JEFE DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN

Funciones. - El Jefe de Sistemas y Tecnologías de la Información se encarga de mantener el correcto funcionamiento de los equipos computacionales, las herramientas informáticas de la empresa y el desarrollo tecnológico de los sistemas de información. Sus responsabilidades son:

- Liderar los Procesos Estratégicos en Tecnologías de la Información alineados a la Misión, Visión y Objetivos de la Empresa.

- Implementación de proyectos, así como investigaciones acerca de la aplicación y uso de las tecnologías de la información y comunicación
- Coordinar el desarrollo de los sistemas de información en función a estudios técnicos relacionados con la determinación de requerimientos reales priorizados como parte de un sistema de información integral y la optimización de los procesos y procedimientos.
- Evaluar y emitir opinión técnica sobre aplicativos informáticos desarrollados por terceros, si fuese el caso, previo a su implementación en las diversas unidades de negocio.
- Planificar, programar, ejecutar y supervisar el mantenimiento preventivo y correctivo según sea el caso de los recursos informáticos: físicos, lógicos y de comunicación.
- Administración de los respaldos de información y la seguridad de los mismos para garantizar la continuidad del negocio en caso de una contingencia.
- Administración de los diferentes servidores y tecnologías con las que cuenta la empresa.

3.8. Procedimiento para la ejecución del modelo.

Una vez acontecido el incidente disruptivo en la unidad de T.I., se detalla los procedimientos a seguir por parte del responsable de llevar a cabo la recuperación de los servicios comprometidos, iniciando con una reunión con los encargados de los servicios afectados, luego se

decide si existe la necesidad de convocar a todos los miembros del comité.

3.8.1. Procesos y lineamientos.

Para poder realizar la ejecución del modelo se definen lineamientos que nos ayuden a la aplicación del Plan de Recuperación ante desastres, a continuación, se procede a detallarlas:

Antes de la eventualidad:

- Se debe disponer de un Coordinador del DRP, responsable de guiar la aplicación del plan.
- Se debe contar con personal altamente calificado de los servicios que administran.
- La corporación debe de aprobar el DRP.
- Disponer de una infraestructura alterna que permita la operación de los diferentes servicios.
- Mantener actualizado el DRP, por lo menos una vez al año.
- Dar a conocer el DRP a toda la unidad de T.I.
- Capacitar continuamente a los integrantes de la unidad de T.I. para afrontar las eventualidades.
- Mantener reuniones con los miembros del comité sobre la responsabilidad de cada uno en el DRP.

- Realizar periódicamente ensayos de la aplicación del DRP.

Durante la eventualidad:

Ocurrido el evento disruptivo, el coordinador del DRP, debe de llamar a los demás integrantes e informar del lugar y hora para la reunión.

- El incidente puede ser manejado mediante el plan de recuperación ante desastres, en el centro de cómputo principal, levantado por los proyectos de disponibilidad y redundancia de la Infraestructura Tecnológica, o mediante servicios brindados por una infraestructura alterna para la continuidad de los servicios de TI.
- Con anterioridad se llegó al compromiso y asistencia de todos los integrantes de la Unidad de TI, en el cual tienen que ser partícipes de la recuperación de los servicios de TI, descritos en el plan de recuperación.
- Los jefes y gerentes departamentales escogerán las personas idóneas, quienes participarán y aportarán con la información necesaria para recuperar la operación de servicios necesarios.
- Si no se contara con las personas idóneas para la ejecución del DRP, el coordinador conjuntamente con un representante del departamento de Recursos Humanos asignará a empleados de rango alto de cada área y que puedan asumir el rol correspondiente.

- El coordinador junto a los demás miembros del comité de recuperación, analizarán y valorarán la afectación de los servicios. En base a este análisis y valoración, planificarán las actividades para la recuperación de los servicios, así como el desarrollo del plan, qué unidades administrativas se trasladarán físicamente a otras oficinas y la decisión de activar los servicios de TI de la infraestructura alterna.
- La monitorización de los procesos de recuperación será controlada por el Coordinador de manera global y por los miembros del comité en los procesos de recuperación que le correspondan.
- El coordinador, tomando en cuenta el estado de excepción por la eventualidad y para agilizar la reparación y recuperación, facilita la adquisición de equipos, servicios y toda provisión necesaria con respecto a TI. También informa continuamente al equipo de manejo de crisis el avance y seguimiento de la recuperación.
- El Gerente de TI, en base al plan establecido, coordina la activación de la infraestructura alterna, será el encargado de supervisar el desarrollo de los procedimientos necesarios en coordinación, monitoreo y control de la recuperación de los servicios de TI.

Después de la eventualidad:

Una vez concluida la eventualidad, el coordinador del DRP revisará cada uno de los procesos ejecutados en el plan.

- Los miembros que intervienen en la ejecución del DRP, mantendrán la debida confidencialidad sobre los documentos que manejen durante la eventualidad.
- En el supuesto de utilizar infraestructura alterna, el coordinador del DRP con la ayuda de los otros miembros del comité, evaluarán los procesos requeridos para regresar a la infraestructura principal.
- El miembro responsable del servicio afectado, ejecutará lo siguiente para desactivar los procesos del incidente:
 - 1) Revisar la infraestructura principal, que todo haya sido reparado y los servicios funcionen correctamente.
 - 2) Revisar el restablecimiento de los sistemas y aplicativos en la infraestructura principal.
 - 3) Comprobar el acceso a los sistemas y aplicativos por los usuarios de la corporación.
 - 4) Coordinar la desactivación de la infraestructura alterna.
 - 5) Revisar el correcto funcionamiento y desempeño de los sistemas y aplicativos de la infraestructura principal.
 - 6) Revisar las actividades relacionadas a la ejecución de respaldos de la infraestructura principal, luego de desactivado el plan.

- El coordinador del DRP deberá disponer la ejecución de la auditoría sobre la aplicación del DRP.
- El coordinador del DRP deberá disponer la recolección de datos referentes a los daños generados en la eventualidad.
- Los miembros del comité analizan y evalúan los resultados obtenidos y plantean de ser necesario ajustes al DRP.
- El coordinador del DRP realizará el informe para presentar al comité de crisis.

CAPÍTULO 4

ANÁLISIS Y DISEÑO DEL PLAN DE RECUPERACIÓN ANTE DESASTRES

Para la aplicación de esta tesis, se ha utilizado la norma ISO 22301:2012 la cual cubre un tema muy extenso como es la continuidad del negocio y dentro de ella la recuperación de los procesos y operaciones en la corporación, esto último aplicable para el desarrollo del DRP planteado en el presente tema de titulación; orientándose en las actividades del área de TI de mayor importancia que mantiene los procesos críticos y comerciales de la empresa.

El plan de recuperación ante desastres tiene como objetivo la continuación de los procesos que ejecuta la unidad de TI de AMCO, que a su vez sirven de apoyo a los otros procesos que se ejecutan en los diferentes departamentos de la organización; los cuales deben estar continuamente a disposición de sus usuarios, garantizando el equilibrio económico y financiero y su subsistencia frente a sus competidores, para cumplir con los requisitos y observaciones que exige la ley.

El plan de recuperación ante desastres está formado por un conjunto de documentos tomando en cuenta las diferentes necesidades de la corporación, los cuales se detallan a continuación:

4.1. Procedimiento para control de documentos y registros

Esta documentación tiene como objetivo certificar la información que se crea y actualiza, tomando en cuenta su identificación, descripción, formato, medios, revisión y aprobación; asegurando su disponibilidad y buen uso cuando se la requiera. Los beneficiarios de este documento son todos los empleados de la organización. **Ver Anexo 1. Procedimiento para control de documentos y registros**

4.2. Plan del Proyecto

La finalidad del plan de proyecto es la definición del propósito para la implementación del plan de recuperación ante desastres, los documentos que se elaborarán, plazos, términos, cargos y responsabilidades del proyecto. Los beneficiarios de esta documentación son la alta dirección y los que conforman el equipo del proyecto. **Ver anexo 2. Plan del proyecto**

4.3. Procedimiento para identificación de requisitos

En el presente documento se determinará las partes interesadas, así como sus necesidades y requerimientos, tomando en cuenta sus requisitos legales aplicables; todo en relación con la continuidad de sus operaciones. Los beneficiarios de este documento son todos los empleados de AMCO. **Ver Anexo 3 Procedimiento para identificación de requisitos**

Lista de requisitos legales, normativos y contractuales.

Esta lista determina los requisitos, los documentos que impone el requisito (la ley o norma), las personas responsables del cumplimiento, los plazos y las personas interesadas. **Ver Anexo 3.1 Lista de requisitos legales, normativos y contractuales.**

4.4. Política para la recuperación ante desastres.

La finalidad de esta política es delimitar el objetivo, alcance y normas básicas para la gestión del plan de recuperación ante desastres. Los beneficiarios son todos los empleados de AMCO, así como sus proveedores y socios que tengan alguna función en el DRP. **Ver Anexo 4. Política para la recuperación ante desastres**

4.5. Metodología para el análisis del impacto en el negocio.

El objetivo de esta documentación es la definición de su metodología para la evaluación de los impactos en la interrupción de las actividades de AMCO, determinando prioridades y objetivos de recuperación. Los beneficiarios de este documento son todos los empleados de AMCO que participan en el DRP. **Ver Anexo 5. Metodología para el análisis del impacto en el negocio.**

4.5.1. Cuestionario sobre el análisis del impacto en el negocio – Servicios de Telecomunicaciones.

En el presente escrito se detalla información general, descripción, impacto general, impacto financiero necesarios para poder recuperar la continuidad de los servicios principales de telecomunicaciones (Internet, enlace, telefonía IP, correo,

etc.). Ver **Anexo 5.1. Cuestionario sobre el análisis del impacto en el negocio – Servicios de Telecomunicaciones.**

4.5.2. Cuestionario sobre el análisis del impacto en el negocio – Sistemas y aplicativos de AMCO.

El objetivo de este documento es detallar la información general, descripción, impacto general, impacto financiero necesarios para poder recuperar la continuidad de los sistemas y aplicativos de AMCO. Ver **Anexo 5.2. Cuestionario sobre el análisis del impacto en el negocio – Sistemas y aplicativos de AMCO.**

4.6. Estrategia de recuperación ante desastres.

El objetivo de este documento es determinar una estrategia adecuada para la recuperación, garantizando cumplir todas las condiciones para reanudar las actividades prioritarias ante el caso de un desastre u otro incidente disruptivo. Constituye la base para preparar el los planes de recuperación de los servicios principales. Ver **Anexo 6 Estrategia de Recuperación de Desastres.**

4.6.1. Lista de actividades

La finalidad de este documento es detallar las actividades primordiales y complementarias de recuperación que aseguren que las operaciones se reanuden en la Unidad de TI. Ver **Anexo 6.1 Lista de Actividades**

4.6.2. Prioridades de recuperación para las actividades

Con este documento se define las interrupciones máximas aceptables para cada actividad y establece prioridades en

consecuencia. Ver **Anexo 6.2. Prioridades de recuperación para las actividades**

4.6.3. Objetivos de tiempo de recuperación para las actividades

El documento detalla los objetivos de tiempos de recuperación para cada actividad dentro del DRP. Ver **Anexo 6.3. Objetivos de tiempo de recuperación para las actividades.**

4.6.4. Ejemplos de escenarios de incidentes disruptivos

En este documento define ejemplos de los escenarios más comunes ocurridos que pueden interrumpir las actividades normales de AMCO. Ver **Anexo 6.4. Ejemplos de escenarios de incidentes disruptivos.**

4.6.5. Plan de preparación para la continuidad de los servicios de TI.

En este documento se enlista los preparativos para cumplir con las condiciones que puedan retornar en forma satisfactoria las actividades de la unidad de TI. Ver **Anexo 6.5. Plan de preparación para la continuidad de los servicios de TI.**

4.6.6. Estrategia de recuperación - Disponibilidad de los servicios de telecomunicaciones

En este documento se definen los responsables de las tareas, los recursos con su tiempo de recuperación y el procedimiento a aplicar para las copias de seguridad tomadas para la recuperación en los servicios de telecomunicaciones. Ver **Anexo 6.6. Estrategia de recuperación – Disponibilidad de los Servicios de Telecomunicaciones.**

4.6.7. Estrategia de recuperación - Disponibilidad de Sistemas y aplicativos de AMCO:

En este documento se definen los responsables de las tareas, los recursos con su tiempo de recuperación y el procedimiento a aplicar para las copias de seguridad tomadas para la recuperación de los sistemas y aplicativos de AMCO. Ver **Anexo 6.7. Estrategia de recuperación – Disponibilidad de Sistemas y aplicativos de AMCO.**

4.7. Plan de recuperación ante desastres.

El presente documento tiene como finalidad la gestión de los incidentes al presentarse un desastre o incidente disruptivo y como se recuperarán las actividades en los tiempos establecidos. Los beneficiarios de este documento son todos los miembros del personal, internos y externos, que cumplan alguna función en el plan. Ver **Anexo 7. Plan de recuperación ante desastres.**

4.7.1. Plan de respuesta a los incidentes.

El objetivo del presente documento es el aseguramiento en términos de salud y seguridad de las personas de cara a una catástrofe u otra calamidad, además de minimizar posibles daños a la institución. Los beneficiarios de esta documentación son todos los empleados de AMCO. Ver **Anexo 7.1. Plan de respuesta a los incidentes.**

4.7.2. Registro de Incidentes.

Esta documentación tiene como objetivo la clasificación de los incidentes a través de un formato para su respectivo registro

cuando estos aparezcan. **Ver Anexo 7.2. Registro de incidentes.**

4.7.3. Ubicaciones para la continuidad de las operaciones.

El objetivo del presente documento nos brinda las ubicaciones alternativas que nos aseguren la continuidad de las operaciones de T.I. en caso de alguna catástrofe o incidente. **Ver Anexo 7.3. Ubicaciones para la continuidad de las operaciones.**

4.7.4. Plan de Transporte.

El presente documento tiene como objetivo la coordinación del transporte en el caso de que se active el plan. **Ver Anexo 7.4. Plan de Transporte.**

4.7.5 Contactos Claves.

Esta documentación registra los datos de las personas involucradas durante la aparición de un incidente disruptivo. **Ver Anexo 7.5. Contactos Claves.**

4.7.6. Plan de recuperación – Servicio de telecomunicaciones.

El objetivo de esta documentación es la definición precisa de cómo AMCO recuperará su infraestructura y servicios de TI en los tiempos establecidos en el caso de que ocurriese una catástrofe o incidente. **Ver Anexo 7.6. Plan de recuperación – Servicio de telecomunicaciones.**

4.7.7. Plan de recuperación – Servicio de sistemas y aplicativos.

El objetivo de esta documentación es la definición precisa de cómo AMCO recuperará su infraestructura y servicios de TI en

los tiempos establecidos en el caso de que ocurriese una catástrofe o incidente. **Ver Anexo 7.7. Plan de recuperación – Servicio de sistemas y aplicativos.**

CAPÍTULO 5

ESQUEMA DE PRUEBAS Y ANÁLISIS DE RESULTADOS DEL DRP

Concluido el Desarrollo del Plan de recuperación ante desastres para la Unidad de TI de AMCO, se procedieron a hacer pruebas o simulacros tomando como estándar la ISO 22301:2012 que nos va a permitir medir su eficiencia y aplicación ante estos eventos adversos.

El objetivo de estas pruebas es determinar la frecuencia y los métodos de verificación para evaluar la factibilidad de las medidas y de los arreglos para la gestión de la continuidad de las actividades en la Unidad de TI de AMCO, como también para establecer las acciones correctivas necesarias.

Este Plan se aplica a todos los elementos que se encuentran dentro del alcance del Plan de Recuperación ante desastres (DRP). Los usuarios de este documento son todas las personas que cumplen una función en el DRP.

5.1. Pruebas, mantenimiento y revisión del DRP.

Es un documento que informa los periodos con que se hacen las pruebas, así mismo el alcance de las mismas y los responsables, adicionalmente se entrega como se implementaron estos simulacros y como se verificaron para hacer funcionar el DRP. Se revisan los resultados obtenidos encontrando que se cumplan lo estipulado en el DRP para corregir el plan si fuera necesario y registrando estos resultados incluyendo las acciones correctivas y sus recomendaciones. Ver **Anexo 8. Plan de Pruebas mantenimiento y revisión del DRP.**

5.1.1. Informe de pruebas y verificación

Es un documento que informa las pruebas realizadas y verificadas con objetivos que hayan alcanzado o no en la prueba. Ver **Anexo 8.1. Informe de pruebas y verificación.**

5.1.2. Plan de mantenimiento y revisión del DRP

Es un documento en cual se describe un cronograma de revisión y mantenimiento periódicos en el año. Ver **Anexo 8.2. Plan de mantenimiento y revisión del DRP.**

5.1.3. Formulario de revisión postincidente

Este documento está disponible para cuando suceda un incidente fuera de los escenarios planteados inicialmente para que pueda ser incluido en las acciones correctivas del DRP. AMCO cuenta con un sistema de Mesa de Ayuda donde se registran todos los incidentes ocurridos. Ver **Anexo 8.3. Formulario de revisión postincidente**

5.2. Plan de capacitación y concienciación.

Este documento tiene como objetivo preparar a todo el personal que cumple una función en el DRP y pueda cumplirla eficazmente. Detalla la función del usuario dentro del DRP sus conocimientos y habilidades, así como la capacitación que necesitaría su registro y el logro obtenido después de capacitarse. Ver **Anexo 9. Plan de capacitación y concienciación**

5.3. Procedimiento para auditoría interna.

El presente documento tiene como objetivo la descripción de las actividades que tengan relación con la auditoría, como lo son la redacción del programa de auditoría, selección del auditor, realización de auditorías individuales e informes. Ver **Anexo 10. Procedimiento para auditoría interna.**

5.3.1. Programa anual de auditoría interna.

El presente documento tiene como objetivo la redacción de la programación anual de auditorías durante los periodos respectivos. Ver **Anexo 10.1. Programa anual de auditoría interna.**

5.3.2. Informe de auditoría interna.

Presentación del formato para el seguimiento de las auditorías internas ejecutadas al DRP una vez implementado. Ver **Anexo 10.2. Informe de auditoría interna.**

5.3.3. Lista de apoyo de auditoría interna.

Se presenta un formato para el seguimiento de los diferentes requerimientos de la norma con el fin de ejecutar la mejora continua al plan. **Ver Anexo 10.3 Lista de apoyo de auditoría interna.**

5.4. Minutas de Revisión por parte de la dirección.

Formato de revisión del DRP por parte de la alta dirección en fechas planificadas, de esta manera asegurando la mejora continua del plan. **Ver Anexo 11. Minutas de Revisión por parte de la dirección.**

5.5. Procedimiento para medidas correctivas.

El presente documento tiene como objetivo la descripción de las actividades que tienen relación con el inicio, la implementación y el mantenimiento de correcciones, así como las medidas correctivas. **Ver Anexo 12. Procedimiento para medidas correctivas.**

Formulario para medidas correctivas.

Formato de presentación para las medidas correctivas identificadas durante una catástrofe en la aplicación del DRP. **Ver Anexo 12.1. Formulario para medidas correctivas.**

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

6.1. Inconvenientes durante la ejecución del DRP.

En la ejecución del presente plan de recuperación ante desastres de la unidad de T.I. de AMCO, se evidenciaron algunas dificultades, las que detallamos a continuación:

- Poca disponibilidad de tiempo de los integrantes de la Unidad de T.I. y de otros departamentos en sus actividades diarias.
- Carencia de capacitaciones de los que conforman la unidad de T.I.
- Tiempos prolongados durante la implementación del DRP para la Unidad de T.I. de AMCO.
- Inconvenientes presentados en la realización de pruebas piloto en tiempo real.

- Carencias presentadas en la definición de la criticidad de los servicios.
- Poca difusión del plan dentro de la Corporación.
- Eventos externos inesperados que atrasaron la implementación del proyecto.

6.2. Resultados del modelo aplicado.

La aplicación del DRP en la corporación AMCO, proyectaron buenos resultados. Los escenarios aplicados garantizan una recuperación de los servicios de forma satisfactoria, que va de la mano con los objetivos de la corporación. Se detallan a continuación sus principales hallazgos:

- La documentación de la corporación con la que se trabajó presenta su situación actual omitiendo datos considerados sensibles para AMCO.
- Tomar en cuenta los sistemas de respaldo utilizados por AMCO, lo que permite disminuir los riesgos en la pérdida de información.
- Durante la realización del análisis de impacto se evaluaron los diferentes servicios distribuidos por su tipo (telecomunicaciones y sistemas y aplicativos).
- Cada rol dentro del DRP tiene asignado su respectivo backup.
- Por temas de confidencialidad, se omiten algunos sistemas y aplicativos y demás recursos utilizados por la corporación AMCO.

- Conocimientos adquiridos gracias a la investigación de propagación de un malware tipo troyano.
- Los integrantes de la unidad de T.I. dieron respuesta en lapsos establecidos en las caídas en el servicio de telecomunicaciones por hardware con averías.
- Teniendo en cuenta los resultados obtenidos en la aplicación del modelo se corrobora su utilidad para la corporación AMCO.
- Para reforzar la aplicación del modelo, se recomienda su aplicación en escenarios más complejos.
- La administración de toda la documentación del modelo podría utilizar un software especializado para esta tarea.

Partiendo de los resultados obtenidos en las pruebas, se inició con la aplicación de las siguientes mejoras:

- Adquisición de licencias corporativas de antivirus.
- Etiquetado de cables de red para su posterior identificación.
- Adquisición de hardware de respaldo para las telecomunicaciones.
- Coordinar capacitaciones continuas y en horarios flexibles para todos los integrantes involucrados en el plan.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Gracias a las características de aplicabilidad de la norma ISO 22301 y su facilidad para adaptarse a un sinnúmero de organizaciones, el presente trabajo investigativo cumple con los requerimientos de resiliencia exigidos por la corporación AMCO.
2. Es necesario establecer diferencias entre el Plan de continuidad (BCP por sus siglas en inglés) que va dirigido a toda la Corporación y del Plan de Recuperación (DRP por sus siglas en inglés) que contempla a la Unidad de T.I. y su infraestructura, este último sirve como base para la continuidad de los servicios ofrecidos a todos sus clientes y usuarios.
3. Es importante contar con riesgos bien identificados en AMCO, así como sus impactos, debido a que serán considerados para el análisis y posterior aplicación de medidas correctivas.
4. De entre los diferentes estándares existentes en la actualidad referente a la continuidad de las operaciones y a la recuperación ante desastres, el estándar elegido representa la mejor elección para la

unidad de tecnología de la corporación AMCO, corroborándose lo anterior con los diferentes escenarios planteados en los cuales se pudo evidenciar su practicidad y eficacia.

5. Se anexan los documentos utilizados para el desarrollo del Plan de recuperación ante desastres, lo que ayudará significativamente para su aplicación, conocimiento y comprensión del estándar elegido.
6. Gracias a la ayuda y colaboración de la unidad de T.I. de AMCO, además de sus esquemas de disponibilidad y respaldos de información, el desarrollo del presente Plan de Recuperación ante desastres fue exitoso.

Recomendaciones

1. Implementar el presente trabajo de investigación realizado para la unidad de T.I. de la corporación AMCO, para así reforzar la continuidad de los procesos de los sistemas y aplicativos que ofrece esta unidad, y que sustentan las operaciones primordiales de la corporación.
2. Formalizar y dar a conocer el plan de recuperación ante desastres a todos los trabajadores de la corporación poniendo énfasis en las acciones correctivas y la mejora continua que se puede realizar, así como clarificar conceptos de recuperación y prevención ante eventualidades.
3. Dar la respectiva capacitación a todo el personal de la corporación, en especial a los que forman parte de sus respectivos comités, lo que ayudará a lograr destrezas y a su vez experiencias necesarias para la implementación del plan.

4. Aplicar el estándar elegido en los demás departamentos de toda la corporación que ayuden a la continuidad de las operaciones gracias a la implementación de un modelo de gestión para la continuidad del Negocio (BCP por sus siglas en inglés).
5. Actualizar periódicamente el plan de recuperación ante desastres con énfasis en los distintos riesgos que puedan ir apareciendo en la unidad de T.I. de la corporación, identificando la infraestructura que los soporta para la aplicación de acciones correctivas y mejora continua.

BIBLIOGRAFÍA

- [1] L. E. Y. Rodríguez, «PLAN DE CONTINUIDAD BS 25999,» s.f. s.f. 2014. [En línea]. Available: http://www.sisteseg.com/files/Microsoft_Word_-_Articulo_BS_25999_DEF1.pdf.
- [2] Business Continuity Institute, «bsigroup,» 2016. [En línea]. Available: <http://www.bsigroup.com/LocalFiles/nl-nl/iso-22301/Bronnen/Horizon-Scan-Report-2016.pdf>. [Último acceso: 09 07 2016].
- [3] C. J. Cruz y P. V. Jiménez, «Proceso administrativo, planeación, organización, dirección y control,» 10 Agosto 2013. [En línea]. Available: <http://www.grandespymes.com.ar/2013/08/10/proceso-administrativo-planeacion-organizacion-direccion-y-control/>.
- [4] E. Mifsud, «Introducción a la seguridad informática,» 26 Marzo 2012. [En línea]. Available: <http://recursostic.educacion.es/observatorio/web/en/software/software-general/1040-introduccion-a-la-seguridad-informatica?showall=1>.
- [5] P. Loza, «Desastres naturales inesperados,» s.f. s.f. 2013. [En línea]. Available: <http://www.iadb.org/es/acerca-del-bid/desastres-naturales-inesperados,6675.html>.
- [6] ICETEX, «MANUAL DE ADMINISTRACION DEL PLAN DE CONTINUIDAD DE NEGOCIOS,» 30 Mayo 2013. [En línea]. Available: https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manual_continuidad_negocio.pdf.

- [7] OSIATIS, «ITIL,» 20 Noviembre 2015. [En línea]. Available: http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/gestion_de_incidentes/introduccion_objetivos_gestion_de_incidentes/introduccion_objetivos_gestion_de_incidentes.php.
- [8] STUDYLIB, «STUDYLIB - Produccion de contenido en Auditoria para Vesprinil,» 2015. [En línea]. Available: <http://studylib.es/doc/310798/produccion-de-contenido-en-auditoria-para-vesprinil>.
- [9] Federacion Internacional de sociedades de la Cruz Roja, «Federacion Internacional de sociedades de la Cruz Roja,» 5 Abril 2016. [En línea]. Available: Recuperado de: <http://www.ifrc.org/es/introduccion/disaster-management/sobre-desastres/que-es-un-desastre/>.
- [10] Observatorio Iberoamericano de protección de datos, «Observatorio Iberoamericano de protección de datos,» 19 Mayo 2014. [En línea]. Available: <http://oiprodat.com/2014/07/28/draas-la-recuperacion-de-desastres-como-servicio-en-el-cloud/>.
- [11] Instituto tecnológico de Sonora, «Introducción a los Sistemas de Información,» 23 Junio 2015. [En línea]. Available: biblioteca.itson.mx/oa/dip_ago/introduccion_sistemas/p3.htm.
- [12] EcuRed, «EcuRed: Conocimiento con todos y para todos,» 28 Mayo 2016. [En línea]. Available: http://www.ecured.cu/Sistema_inform%C3%A1tico.
- [13] P. Aguilera López, «Seguridad informática,» 1 Junio 2010. [En línea]. Available:

<https://books.google.com.ec/books?id=Mgvm3AYIT64C&pg=PA23&dq=Un+instru#v=onepage&q&f=false>.

- [14] Revista Gerencia, «GOBIERNO DE TI: Para obtener el mayor valor de las Tecnologías de Información,» Agosto 2013. [En línea]. Available: <http://www.emb.cl/gerencia/articulo.mvc?xid=3261&sec=14>.
- [15] SANS Institute, «Introduction to Business Continuity Planning,» 2013 Agosto 2013. [En línea]. Available: Recuperado de: <https://www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559>.
- [16] TecLaw, «¿Qué es un plan de contingencia en seguridad informática?,» 14 Junio 2006. [En línea]. Available: <http://pumarino.blogspot.com/2006/06/qu-es-un-plan-de-contingencia-en.html>.
- [17] N. Sanchez, «CELINGEST,» 1 Marzo 2013. [En línea]. Available: <http://blog.celingest.com/2013/03/01/recuperacion-desastres-disaster-recovery/>.
- [18] M. A. Mendoza, «welivesecurity,» 14 Octubre 2014. [En línea]. Available: <http://www.welivesecurity.com/la-es/2014/10/14/plan-de-recuperacion-ante-desastres/>.
- [19] Universidad de Caldas, «BCM Business continuity management, BS 25999, BCI (Business continuity institute),» 2010. [En línea]. Available: https://auditoriauc20102mivi.wikispaces.com/file/view/BCM_BS+25999_BCI201021700620355.pdf.
- [20] ISO 22301, Seguridad de la Sociedad: Sistemas de Continuidad del

Negocio, ISO, 2012.

[21] AENOR, «AENOR30,» 25 Agosto 2015. [En línea]. Available: https://www.aenor.es/aenor/certificacion/seguridad/gestion_continuidad_negocio.asp#.V2_1-zVT4sw.

[22] ISO 27001, Tecnología de la Información - Técnicas de Seguridad Sistemas de Gestión de la Seguridad de la Información - Requisitos., ISO, 2013.

[23] D. Kosutic, «www.advisera.com,» 08 04 2015. [En línea]. Available: <https://advisera.com/27001academy/iso-27001-22301-premium-documentation-toolkit/>.

[24] D. Kosutic, «27001 ACADEMY,» 16 10 2016. [En línea]. Available: <https://advisera.com/27001academy/>

GLOSARIO DE TÉRMINOS

ACTIVO/ACTIVO: En informática se refiere a dos equipos que continen el mismo servicio, a los cuales los clientes pueden conectarse indistintamente. Dentro de TI hace referencia a dos equipos con el mismo servicio, sin embargo, los clientes pueden conectarse al equipo pasivo únicamente cuando el equipo activo se encuentre fuera de servicio.

BACKUP: En tecnologías de la información (abreviado TIC) se refiere a una copia de los datos informáticos originales, se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.

BCM: Por sus siglas en inglés “Business Continuity Management”, es un proceso de gestión integral, identifica potenciales impactos de una amenaza y provee estructuras de respuesta que resguarde los intereses de las empresas.

BCP: “Business Continuity Plan”, es el plan para recuperar y restaurar las operaciones críticas parcial o totalmente, luego de interrumpidas por un incidente disruptivo.

DRP: Es un plan de recuperación de desastres, consiste en un conjunto de procedimientos para recuperar y proteger la infraestructura tecnológica de una empresa en caso de un desastre.

FIREWALL: Es un sistema (físico o virtual) de Seguridad Informática, permite controlar y proteger el tráfico de datos de una red de computadores.

INCIDENTE DISRUPTIVO: Se refiere a una interrupción o ruptura brusca de una actividad o servicio.

IPS: “Intrusion Prevention System”, son sistemas dedicados a la prevención de intrusiones a partir de la identificación y bloqueo de ataques en el tránsito de la red. Por lo general son sistemas robustos de hardware y software

LAN: Son las siglas en inglés para “Local Area Network”, es un grupo de equipos que están conectados dentro de un área geográfica pequeña.

PDCA: El nombre del Ciclo PDCA viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés “Plan, Do, Check, Act”. También es conocido como ciclo de mejora continua o Círculo de Deming.

ROUTER: Es un dispositivo de red informática, permite el enrutamiento de paquetes entre redes independientes.

RPO: “Recovery Point Objective”, determina la máxima cantidad de información que se puede perder, es el tiempo máximo establecido de la última copia de seguridad de los datos de la empresa, respecto a la anterior copia.

RTO: “Recovery Time Objective”, es el tiempo objetivo para la reanudación de los servicios tecnológicos después de un desastre.

SAN: “Storage Area Network”, es una red diseñada para interconectar servidores, librerías, permitiendo el tránsito de datos sin afectar a las redes por las que acceden los usuarios.

SGCN: Sistema de Gestión de Continuidad del Negocio, es un proceso integral de gestión que identifica los posibles impactos que amenazan a una organización, y ofrece un marco para disponer de los servicios en todo momento.

SGSI: Es la abreviatura utilizada para referirse a un Sistema de Gestión de Seguridad de la Información.

SWITCH: Dispositivo electrónico utilizado en redes de Computadoras LAN, permite interconectar varios equipos que conforman una red informática.

TICs: Se refiere a las Tecnologías de la Información y la Comunicación

VPN: Siglas en inglés de “Virtual Private Network”, es una tecnología de red, se establece entre 2 sitios lejanos mediante Internet, formando una red privada.

WAN: “Wide Area Network”, es una red de área amplia, abarca un área geográfica relativamente grande.