UNIVERSIDAD ACCIÓN PRO EDUCACION Y CULTURA
(UNAPEC)

Decanato de Ingeniería e Informática
Escuela de Informática

Plan de Recuperación de Desastres (DRP) para el área de TI
Caso: Empresa Quimidomsa

Sustentantes:

Ryan Corominas **2002-2021**

Okelarys Sánchez **2003-0139**

Asesores:

Ing. Ramón Gómez

Lic. Antonio Calderón

Monografía para optar por el título de Ingeniero en Sistemas de Computación

Distrito Nacional, República Dominicana

2010

Dedicatoria.

A nuestro sabio y eterno Dios, al único que se merece toda la gloria y la honra. Todos mis logros y conocimientos plasmados en este documento se lo dedico a Él.

"Al Dios y Padre nuestro sea gloria por los siglos de los siglos. ***Amén."***

Filipenses 4:20

Agradecimientos

A Dios, gracias por permitirme completar esta carrera, dándome los conocimientos y las fuerzas necesarias para lograrlo. Tuya es toda la gloria.

A mis padres, gracias por inculcarme en el camino correcto y ser ejemplos a seguir para continuar toda esta larga etapa.

A mi Novia, por tu ayuda idónea, por darme siempre ánimo para continuar y por tu paciencia en el transcurso de todo el monográfico.

A los Asesores, gracias a cada uno de ellos por su disponibilidad, dedicación y apoyo para lograr esta meta.

A todos mis familiares y amigos, gracias por su apoyo y motivaciones, gracias por todas sus oraciones.

Ryan Armando Corominas Marmol

Agradecimientos

Dicen que la guerra no consiste solo en la batalla sino en la voluntad de contender; Al concluir esta etapa de mi vida deseo agradecer a aquellas personas que me ayudaron a mantener firme mi voluntad aún cuando ya mis esfuerzos no me bastaban:

Mi familia, gracias por ser mi motivación e impulsarme día a día a luchar por mis metas, en la vida todo es posible si se lucha con el corazón.

Mi novia y su familia, su preocupación, paciencia y ánimos me fueron de gran ayuda sobre todo en los momentos finales, cuando la carga se hacía más difícil.

Dios, Mis sentidos y mi caminar están prestos a ti, un simple gracias no es suficiente.

Okelarys Rafael Sánchez Soto

Resumen

En la actualidad muchos negocios dependen fuertemente de la tecnología y sistemas automáticos y la interrupción de estos, por inclusive unos cuantos días podría causar serias pérdidas financieras y poner en peligro su supervivencia. La continuidad de las operaciones de una organización depende de la conciencia administrativa acerca de desastres poderosos, así como su habilidad para desarrollar planes para minimizar las interrupciones de las funciones esenciales.

El siguiente monográfico consistirá en la creación Un plan de recuperación de desastres y sus acciones consecuentes que se deben realizar antes, durante y después del desastre. Este plan debe ser probado y registrado para asegurar la continuidad de las operaciones y la disponibilidad de los recursos necesarios en caso de desastre.

En primer lugar, conoceremos la empresa a realizar el plan, realizando evaluaciones y análisis para identificar las amenazas de la empresa y al igual identificar los procesos críticos del negocio. Estas informaciones recopiladas nos darán un marco a seguir para la elaboración de estrategias que contrarrestaran las amenazas de cualquier desastre que podría ocurrir.

La planeación de recuperación de desastres tiene como objetivo proteger a la organización en caso de que sus operaciones y/o servicios críticos computacionales se interrumpan. La clave consiste en la preparación del plan. En este sentido se garantizara una buena continuidad de negocios cuando la implementación fue bien desarrollada. Posterior a esto es necesario que exista un plan de mantenimientos y pruebas, todas las actualizaciones del plan de recuperación de desastres deben estar debidamente estructuradas y controladas. Además, cada vez que se realizan cambios en el plan deben ser completamente probado, y los cambios adecuados deben tomarse en cuenta para los materiales de formación. Entrenar al personal en los procedimientos particulares es un proceso vital a seguir durante el proceso de recuperación del negocio.

Introducción

Los ataques informáticos, las inclemencias climitas, y los conflictos de carácter social son los males que impactan las actividades de las compañías de hoy en día, ¿está su negocio preparado para tolerar una de estas situaciones? Es la pregunta que la mayoría de empresarios, gerentes y accionistas se realizan, otra pregunta interesante es ¿Podrá su negocio volver a operar luego de haber sufrido un desastre?, Si se ha estado realizando estás preguntas y sus respuestas son un tanto desmotivadoras, entonces debe empezar a cambiar su esquema de trabajo y prepararse para la continuidad de su negocio.

Gestión de continuidad del negocio es un esquema de trabajo que provee de la habilidad y preparación para manejar las interrupciones del negocio, con el objetivo de proveer la continuidad de los servicios a un nivel mínimo aceptable y así salvaguardar la posición financiera y competitiva a corto y largo plazo.

Bajo este esquema hemos realizado la propuesta de un Plan de recuperación de desastres para el área de tecnología de información contenido en este documento a la empresa Químicos Dominicanos S.A (Quimidomsa) con el objetivo de proveerle de la estructura y preparación necesaria para recuperar los procesos críticos en un corto tiempo, ante la posibilidad de presentarse algún incidente que provoque una interrupción de las operaciones.

Capitulo 1: Introducción del Proyecto

Introducción del proyecto

El auge de la tecnología de información en los negocios ha encadenado una dependencia casi total de los sistemas de información en la mayoría de los procesos y actividades de las organizaciones. Por este motivo, las organizaciones requieren de sus sistemas, datos y sus informaciones relevantes pueden ser preservados, aunque no todas las organizaciones han implementado un plan que le provea la capacidad para restablecer las operaciones de TI y de negocio, ante eventos que pudieran interrumpir el cumplimiento de lograr sus objetivos estratégicos.

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

Por esta dependencia de TI, cualquier falla podría causar serias pérdidas financieras y poner en peligro la supervivencia de cualquier organización. Para contrarrestar cualquier amenaza debemos contar con un adecuado plan que reduzca el tiempo de interrupción de los servicios de TI y garantice la recuperación el flujo de información de la organización.

1.2 Antecedentes de la empresa

La empresa Químicos Dominicanos S.A. (Quimidomsa), fundada en 1985 comenzó sus operaciones como fabricante de materias primas para la industria de pinturas, convirtiéndose rápidamente en el suplidor por excelencia del mercado local en República Dominicana.

Luego de varios años de crecimiento constante, sus actividades comerciales se expanden en 1992 iniciando actividades de exportación comenzando por Haití y Puerto Rico, alcanzando posteriormente una marcada participación en mercados de Centroamérica y Caribe.

Siguiendo con su actividad de expansión, se adquiere en el año 2009 el negocio de dispersiones poliméricas en Guatemala, incorporando la tecnología y las prestigiosas marcas a la gama actual de productos, con lo que con esta adquisición se afianza el liderazgo tecnológico y productivo de Quimidomsa en la región.

Misión

Su misión es producir y comercializar resinas sintéticas de excelente calidad a través de la constante innovación y búsqueda de las mejores tecnologías aplicables a sus mercados, con el objeto de satisfacer las necesidades de sus clientes a través de una esmerada atención comercial, que nos posicione como la opción preferida de los mismos.

Para eso cuentan con un equipo de trabajo competente, comprometido y motivado.

Sus clientes y proveedores no sólo son sus socios comerciales, son sus amigos, con los cuales buscamos constituir relaciones de mutuo beneficio y largo plazo a través de una constante innovación y creatividad que nos garanticen un crecimiento sostenido.

Visión

Como organización nuestra visión es ser la empresa líder en la producción y comercialización de resinas sintéticas en Centroamérica y el Caribe, con los más altos niveles de calidad, excelencia, eficiencia y seguridad, con el fin de satisfacer y en lo posible superar las expectativas de sus clientes.

Entre sus productos están:

Aditivos

Una serie de aditivos completan la paleta de productos de QUIMIDOMSA para la correcta formulación de sus pinturas al látex.

Normalmente los espesantes de tipo HASE, se emplean en pinturas de bajo PVC, o sea alto contenido de dispersiones poliméricas, ya que el espesamiento ocurre por interacción entre la emulsión y el espesante propiamente dicho.

Adhesivos

QUIMIDOMSA produce y comercializa en sus plantas de República Dominicana y Guatemala materias primas para la fabricación de adhesivos, ofreciendo una gama muy amplia de posibilidades para producir todo tipo de adhesivos base acuosa, para el pegado de papel kraft, madera, etiquetado sobre sustratos plásticos como PVC o PET, encolado de libros.

La marca de QUIMIDOMSA para los adhesivos "Ready to use", que abarcan desde adhesivos para uso escolar elaborado con materias primas inocuas y libre de solventes para el contacto con los niños, agentes de barrera de humedad para las cajas de cartón corrugado que se emplean en el embalaje de frutas y toda la gama de adhesivos para papel tissue.

Construcción

También en construcción QUIMIDOMSA ofrece una variedad de soluciones que abarca la posibilidad de modificar morteros, y cementos a través de nuestros productos y las excelentes propiedades de las resinas vinil maleato o vinil VeoVa que resultan ideales para estas aplicaciones.

Finalmente los productos completan la gama de productos que permiten formular pinturas elastoméricas de alto desempeño, excelente elongación y excelentes propiedades de recuperación tanto para techos como paredes.

Pinturas y Recubrimientos arquitectónicos

Nuestra gama de productos va desde dispersiones vinil acrílicas de excelente perfomance que recomendamos para pinturas interiores, dispersiones estireno acrílicas de excelente resistencia al frote húmedo que pueden usarse en pinturas para interiores y exteriores, para formular pinturas para pisos deportivos, pinturas para demarcación vial, donde se requiere una muy alta resistencia alcalina y pinturas elastoméricas con sobresalientes propiedades de elongación.

La combinación con resinas poliuretánicas nos permite incluso formular lacas para muebles y barnices para pisos de parquet.

1.3 Objetivos de la investigación.

a. Objetivo general.

Diseñar e implementar un plan de recuperación de desastre para el área de TI de la empresa Quimidomsa.

b. Objetivos específicos.

- Analizar todos los procesos actuales con la finalidad de revisar si existen vulnerabilidades y riesgos en alguno de estos.
- Analizar los procesos críticos de la empresa y los de mayor prioridad.
- Definir roles a cada persona que tendrán responsabilidades en el proceso de recuperación del área de TI.
- Elaborar Políticas y normas para el personal de TI en relación al cumplimento y acople del plan de recuperación.
- Capacitar y concientizar al personal sobre el plan de recuperación implementado.

1.4 Descripción del proyecto

Cada día aumenta la demanda de información y la realización de los procesos y actividades de la empresa con rapidez y eficiencia, esto a su vez ha creado una dependencia de la tecnología de información en las empresas. Es por ello que se hace imprescindible para las mayorías de las empresas contar con una continuidad de negocios, donde puedan asegurar la disponibilidad de servicios en cualquier catástrofe o situación que pueda afectar esta continuidad, ya que la tendencia del mercado actual son compañías que ofrezcan servicios 24 horas o 24/7 de acuerdo a lo requerido.

Un estudio realizado por Comunicaciones World, demostró que solo un 15% de las empresas Españolas está capacitada para recuperarse de posibles desastres; Para evitar cualquier situación que pueda dejar sin funcionamiento a los sistemas informáticos, cerca de un 11% de las empresas consultadas tienen implementados algún tipo de plan

de contingencia que aseguren la continuidad y la recuperación de los sistemas. Por otra parte un 34% de las empresas han matizado que tienen desarrollado un plan de contingencia de modo orientativo.

El 56% de las empresas entrevistadas tiene elaborado un plan de recuperación de la información, pero sólo el 15% lo tiene hecho de forma documentada y detallada y el 41% restante lo tiene elaborado sólo de modo orientativo. El 29% de las empresas, aunque no lo tengan elaborado, tiene previsto hacerlo y el 10% de las empresas ni siquiera tiene previsión de realizarlo. Estos datos indican que si se generara algún tipo de desastre, sólo un 15% de las empresas estaría capacitado para recuperarse de las diferentes pérdidas.

Por poner otro ejemplo, reportes del Centro Nacional para la Prevención contra Desastres de México (Cenapred) indican que los huracanes Emily, Stan y Wilma en México dejaron pérdidas aproximadas de 45,000 Millones de pesos, cifra que, a decir del organismo, es seis veces mayor al promedio histórico que tiene el país por desastres de diversa índole.

Si analizamos a nuestro país, según un estudio realizado por la Asociación Dominicana de Mitigación de desastres, República Dominicana ha sido impactada desde el año 1900 al 2004 (104 años) por fenómenos de magnitud desastrosa. Los fenómenos naturales que más han atacado el país son los siguientes:

- 20 huracanes, 7 de ellos muy intensos.
- 8 inundaciones
- 4 sismos.

Refiriéndonos a estos fenómenos, han dejado un saldo aproximado de 10,606 pérdidas humanas; daños económicos estimados en 109 millones de pesos (Al año 2004 - 234 mil dólares); afectando directamente a 20 mil quinientos noventa y cinco personas.

Las cifras presentan variaciones entre este estudio y otros de la misma índole, porque en cada caso, lamentablemente, en el país no se cuenta con las herramientas necesarias para realizar un adecuado levantamiento de la información.

Un Plan de Continuidad del negocio (BCP) resulta de una metodología aplicada al interior de la empresa y se usa para crear planes logísticos sobre cómo una organización debe recuperar y restaurar sus funciones críticas de manera parcial o total después de sufrir una interrupción por un desastre o situación inesperada. También sirve para que la organización esté lista para futuros incidentes que puedan ponerla en peligro.
Por su parte, un Plan de Recuperación de desastres (DRP) es el proceso de recuperación de datos, incluyendo software y hardware críticos, para que un negocio pueda comenzar de nuevo sus operaciones en caso de una eventualidad de este tipo.

En tal sentido, es necesario implementar para el área de TI de la empresa Quimidomsa un plan recuperación de desastre (DRP). Este plan de DRP aumentará la confianza y seguridad en gran medida al personal del departamento de TI donde tendrán mayor control de la situación de emergencia, teniendo en sus manos las normas y procedimientos y además las herramientas necesarias para contrarrestar cualquier amenaza.

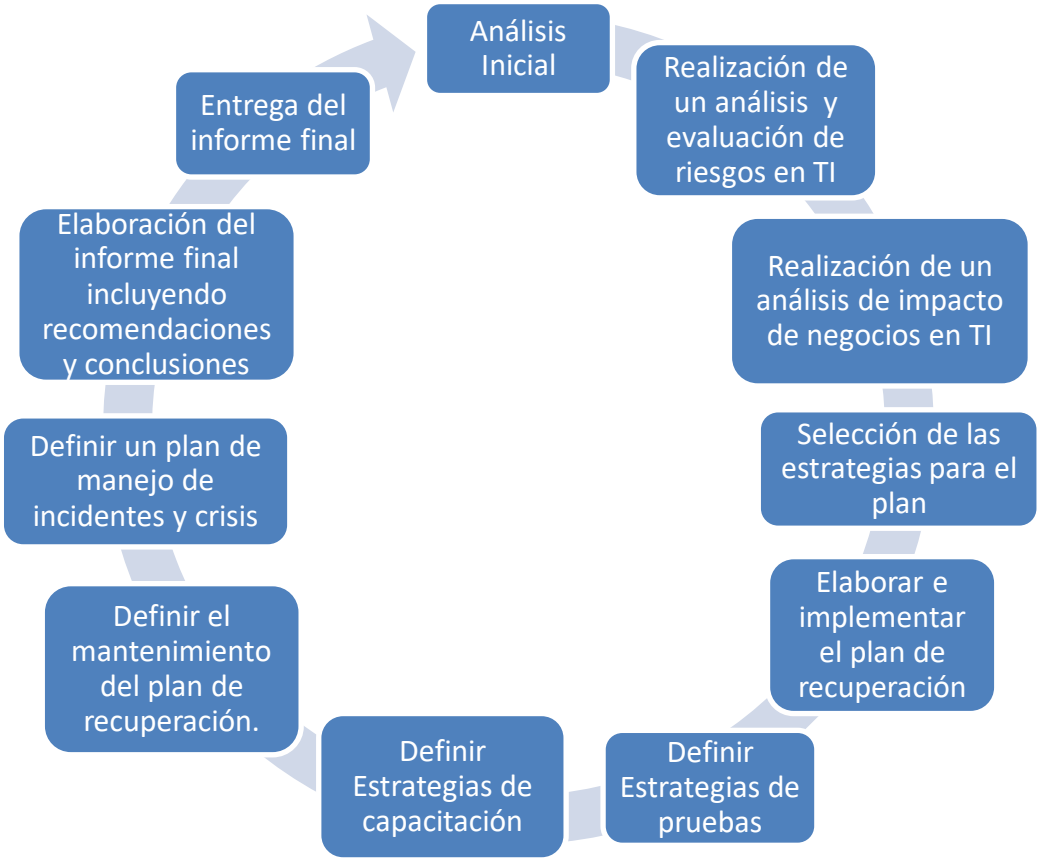
1.5 Alcance del proyecto

El proyecto se desarrolla en la empresa Quimidomsa en la sucursal del municipio de Haina, provincia de San Cristóbal, República Dominicana y en la sucursal de la ciudad de Guatemala, Guatemala. El periodo de ejecución de este proyecto es desarrollado en el intervalo de enero-abril 2010 y enfocados bajo el siguiente esquema de trabajo:

1. **Fase de iniciación y análisis:** Donde se realizará la obtención de datos sobre la empresa, el tipo de estructura y la información que estaremos protegiendo y/o recuperando.
2. **Realización de un análisis y evaluación de riesgos(RA):** Con este análisis atacaremos o minimizaremos todas las vulnerabilidades que pueden convertirse en alguna amenaza para la empresa, Con un enfoque especial en el área de TI.
3. **Realización de un análisis de impacto de negocios (BIA):** Nos permitirá identificar las áreas que sufrirían pérdidas financieras y operacionales, estimando el tiempo de recuperación ante algún desastre.
4. **Realización de la estrategia para el plan de recuperación del área de TI:** Propondremos diversas estrategias acorde a las opciones del mercado para reducir las vulnerabilidades.
5. **Elaborar e implementar el plan de recuperación de desastres para el área de TI:** De acuerdo a las estrategias seleccionadas por la dirección de la organización, realizaremos e implementaremos el plan de recuperación.
6. **Definir Estrategias de pruebas del plan de recuperación:** En esta fase definiremos un esquema para la realización de pruebas, donde indicaremos la periodicidad de las mismas.
7. **Definir Estrategias de capacitación:** Todo la organización debe estar inmersa en la cultura de continuidad y recuperación, Nuestros mayores esfuerzos serán con el personal de TI
8. **Definir el mantenimiento del plan de recuperación:** Asignaremos responsabilidades de actualización y mantenimiento para que el plan se mantenga actualizado al 100% independientemente del cambio que sufra la empresa.

9. **Definir un plan de manejo de incidentes y crisis:** Con este plan trazaremos las pautas de los pasos a seguir ante cualquier incidente ciñéndonos a lo establecido en el plan general de recuperación.
10. **Elaboración del informe final incluyendo recomendaciones y conclusiones:** Elaboraremos un informe final con todos los hallazgos, recomendaciones y conclusiones.
11. **Entrega del informe final:** El único entregable que llevará este proyecto es el informe final que se presentará a la empresa.

Lo indicado anteriormente es expresado en el siguiente gráfico:



1.6 Metodología utilizada en el proyecto

Para este proyecto se utilizaron los siguientes métodos:

- Métodos de Observación: Se realizaron visitas y evaluaciones generales del área de TI, y de toda la estructura organizacional empleando la observación sistemática, es decir anticipando y conociendo de antemano los aspectos en los que hicimos hincapiés en este proceso de observación.

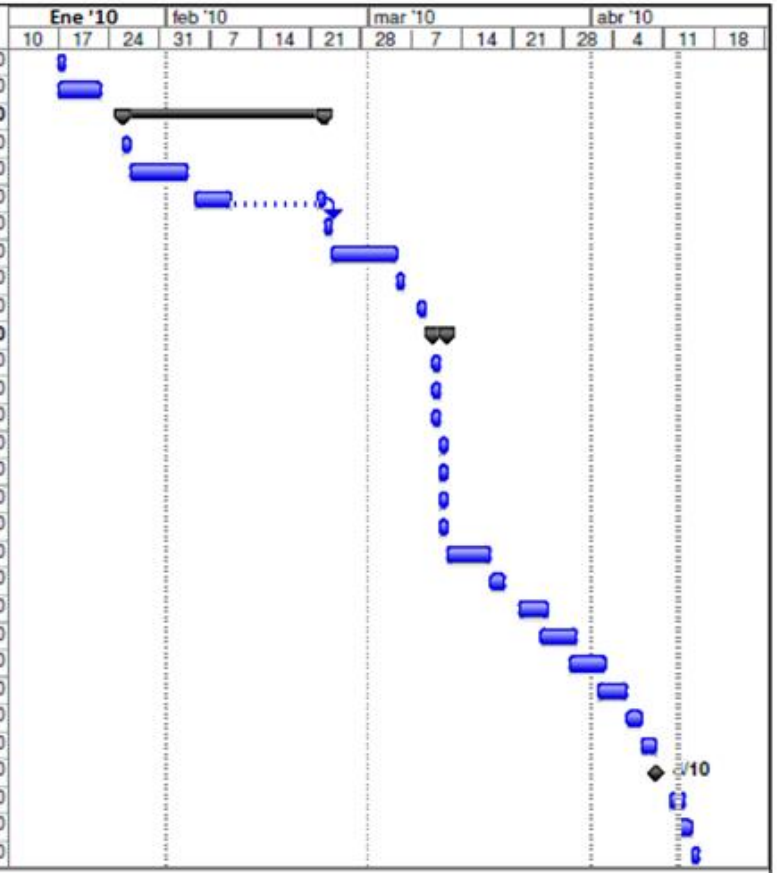
- Métodos de análisis: Utilizamos el análisis con el fin de compilar la información y datos capturados en el proceso de observación, entrevistas y demás, con el fin de que nuestra problemática inicial quede totalmente solucionada o encaminada a hacerlo.

1.7 Equipo del proyecto

Para el desarrollo de este proyecto proponemos el siguiente esquema:

1.8 Cronograma del proyecto

Id	Nombre de tarea	Duración	Comienzo	Fin
1	Selección de Tema	1 día	dom 1/17/10	dom 1/17/10
2	Recopilación de información	6 días	dom 1/17/10	vie 1/22/10
3	**Elaboracion de Anteproyecto**	**21 días**	**mar 1/26/10**	**lun 2/22/10**
4	Selección de Empresa	1 día	mar 1/26/10	mar 1/26/10
5	Investigación Guia de Anteproyecto	6 días	mié 1/27/10	mié 2/3/10
6	Asesorias	4 días	vie 2/5/10	lun 2/22/10
7	Entrega de Anteproyecto	1 día	mar 2/23/10	mar 2/23/10
8	Recopilación de información	7 días	mié 2/24/10	jue 3/4/10
9	Entrevista a Director de Seguridad	1 día	vie 3/5/10	vie 3/5/10
10	Visita a las instalaciones	1 día	lun 3/8/10	lun 3/8/10
11	**Entrevistas y cuestionarios**	**2 días**	**mié 3/10/10**	**jue 3/11/10**
12	Gerente de Ventas	1 día	mié 3/10/10	mié 3/10/10
13	Gerente de Logística	1 día	mié 3/10/10	mié 3/10/10
14	Gerente de Compras	1 día	mié 3/10/10	mié 3/10/10
15	Gerente de Producción	1 día	jue 3/11/10	jue 3/11/10
16	Gerente de finanzas	1 día	jue 3/11/10	jue 3/11/10
17	Gerente de Recursos humanos	1 día	jue 3/11/10	jue 3/11/10
18	Gerente de Tecnología	1 día	jue 3/11/10	jue 3/11/10
19	Identificación amenazas	4 días	vie 3/12/10	mié 3/17/10
20	Elaboración de Controles	2 días	jue 3/18/10	vie 3/19/10
21	Análisis de los procesos de impacto	4 días	lun 3/22/10	jue 3/25/10
22	Definición de estrategias	3 días	jue 3/25/10	lun 3/29/10
23	Desarrollo del Plan	5 días	lun 3/29/10	vie 4/2/10
24	Elaboración de Plan de mantenimientos	2 días	vie 4/2/10	lun 4/5/10
25	Desarrollo de programas de capacitación y difusión	2 días	mar 4/6/10	mié 4/7/10
26	Recopilación de trabajos realizados	2 días	jue 4/8/10	vie 4/9/10
27	Entrega a los asesores para corrección	0 días	sáb 4/10/10	sáb 4/10/10
28	Correciones sugeridas por asesores	2 días	lun 4/12/10	mar 4/13/10
29	Impresión y empastado del documento	2 días	mar 4/13/10	mié 4/14/10
30	Entrega del trabajo final	1 día	jue 4/15/10	jue 4/15/10



Proyecto: Monografico DRP
Empresa: Quimidomsa.
Fecha: del 17/01/2010 al 15/04/2010

Tarea — Hito — Tareas externas
División — Resumen — Hito externo
Progreso — Resumen del proyecto — Fecha límite

Capitulo 2: Evaluación de Riesgos y Análisis de impacto al negocio.

2.1 Evaluación de riesgos (RA) en TI

Objetivo

Con el análisis de evaluación de riesgos, vemos las posibles amenazas (vulnerabilidades) que se puedan presentar en la organización, con el objetivo de minimizarlas y reducir el impacto que esto pueda provocar en la operación normal de la empresa.

Las amenazas siempre han existido y seguirán existiendo, la diferencia es que en algunos casos puede ser más rápida, más difícil de detectar, o mucho más atrevida. Es por esto que toda organización debe estar en alerta y saber implementar sistemas de seguridad basados en un análisis de riesgos para evitar o minimizar las consecuencias no deseadas.

Definición de análisis de riesgo:

Es una actividad centrada en la identificación de fallas de seguridad que evidencien vulnerabilidades que puedan ser explotadas por amenazas, provocando impactos en el negocio, otro concepto interesante sería que es una actividad de análisis que pretende, a través del rastreo, identificar los riesgos a los cuales los activos se encuentran expuestos.

Los resultados que nos arroja el análisis de riesgo nos permite:

- Encontrar la consolidación de las vulnerabilidades para identificar los pasos a seguir para su corrección, minimización o eliminación.
- Identificar las amenazas que pueden explotar esas vulnerabilidades
- Determinar las recomendaciones para que las vulnerabilidades sean corregidas o reducidas.

2.1.1 Determinación los posibles riesgos

¿Qué es el riesgo?

Es la probabilidad de que una amenaza aproveche una vulnerabilidad que provoque un impacto en mis operaciones. Por lo tanto existe una relación entre Vulnerabilidad-Amenaza-Impacto, y está relación es la condición principal a tomar en cuenta en el momento de priorizar acciones de seguridad para la protección o recuperación de los activos. La relación se puede expresar del siguiente modo:

Vulnerabilidades:
Aquellas que son encontradas en la infraestructura o sistemas.

Se convierten en:

Amenazas:
Son los hechos que deben ser evitados en una organización puesto que causan un impacto en el negocio. Las amenazas generan una serie de problemas que pueden afectar los principios de seguridad de la organización.

Producen un:

Impacto:
Que pueden ser desastrosos según su gravedad y amplitud. Sin importar el tipo de amenaza, lo importante es evaluar el impacto que puede causar en los diferentes activos de la empresa.

2.1.2 Determinación de las amenazas

¿Qué es una Amenazas?

s un fenómeno, proceso natural o situación provocada por el ser humano que puede poner en peligro a un grupo de personas, sus bienes y su ambiente.

Las amenazas también se le relaciona con los desastres, en fin una amenaza es todo aquello que:

- Impacte adversamente las operaciones del negocio
- Interrumpa la operación de procesamiento de información crítica (Aunque no todas las interrupciones son desastres)

Tipos de amenazas, desastres o interrupciones

Existen diferentes situaciones que pueden impactar negativamente las operaciones normales de una organización, entre estos, están:

1. Fenómenos naturales
2. Fuego
3. Fallas de energía
4. Ataques terroristas
5. Interrupciones organizadas o deliberadas
6. Sistema y/o fallas de equipo
7. Error humano
8. Virus informáticos
9. Cuestiones legales
10. Conflictos sociales
11. Enfermedades y Epidemias

1. **Fenómenos naturales**

   Los Fenómenos naturales, como la lluvia o el viento, se convierten en desastre natural cuando superan un límite de normalidad, medido generalmente a través de un parámetro. Éste varía dependiendo del tipo de fenómeno (escala de Richter para movimientos sísmicos, escala Saphir-Simpson para huracanes, etc.).
   Los efectos de un desastre natural pueden amplificarse debido a una mala planificación de los asentamientos humanos, falta de medidas de seguridad, planes de emergencia y sistemas de alerta provocados por el hombre se torna un poco difusa.

   A continuación algunos de los desastres naturales más frecuentes.

   - **Avalancha:** Una avalancha es un deslizamiento brusco de material, mezcla de hielo, roca, suelo y vegetación ladera abajo. Las avalanchas pueden ser de piedras o de polvo. Las avalanchas son el mayor peligro durante el invierno en las montañas, pueden recorrer kilómetros, y provocar la destrucción total de la ladera y todo lo que encuentre a su paso.

   - **El Calor:** Es un desastre caracterizado por el calor el cual se considera extremo e inusual en el lugar donde sucede. Las olas de calor son extrañas y necesitan combinaciones especiales de fenómenos atmosféricos para tener lugar, y puede incluir inversiones de vientos, y otros fenómenos.

   - **Deslizamientos de tierra:** Un deslizamiento de tierra es un desastre estrechamente relacionado con las avalanchas, pero en vez de arrastrar nieve, llevan tierra, rocas, árboles, fragmentos de casas, etc. Los corrimientos de tierra pueden ser provocados por terremotos, erupciones volcánicas, lluvias de larga duración. o inestabilidad en la zona circundante.

- **Erupción volcánica** Los volcanes son aberturas o grietas en la corteza terrestre a través de la cual se puede producir la salida de lava, gases, o pueden explotar arrojando al aire grandes bloques de tierra y rocas. Este desastre natural es producido por la erupción de un volcán.

- **El frío:** Los frentes fríos se mueven rápidamente. Son fuertes y pueden causar perturbaciones atmosféricas tales como tormentas de truenos, chubascos, tornados, vientos fuertes y cortas tempestades de nieve antes del paso del frente frío, acompañadas de condiciones secas a medida de que el frente avanza.

- **Granizo:** Una tormenta de granizo es un desastre natural donde la tormenta produce grandes cantidades de granizo que dañan la zona donde caen. Los granizos son pedazos de hielo, las tormentas de granizo son tormentas que precipitan granizos.

- **Huracán:** Un huracán es un sistema tormentoso ciclónico de baja presión que se forma sobre los océanos. Es causado por la evaporación del agua que asciende del mar convirtiéndose en tormenta. El efecto Coriolis hace que la tormenta gire, convirtiéndose en huracán si supera los 110 km/h. En diferentes partes del mundo los huracanes son conocidos como ciclones o tifones.

- **Inundación:** Una inundación es un desastre natural causado por la acumulación de lluvias y agua en un lugar concreto. Puede producirse por lluvia continua, una fundición rápida de grandes cantidades de hielo, o ríos que reciben un exceso de precipitación y se desbordan, y en menos ocasiones por la destrucción de una presa.

- **Terremoto:** Se da en las placas tectónicas de la corteza terrestre. En la superficie, se manifiesta por un movimiento o sacudida del suelo, y puede dañar enormemente a estructuras mal construidas. Los terremotos más poderosos pueden destruir hasta las construcciones mejor diseñadas. Además, pueden provocar desastres secundarios como erupciones volcánicas o tsunamis.

- **Tormenta:** Una tormenta es un ejemplo de tiempo extremo caracterizado por la presencia de rayos, abundante lluvia, fuertes vientos, granizo y en ocasiones nieve y tornados.

- **Tormenta eléctrica:** Es una poderosa descarga electrostática natural producida durante una tormenta. La descarga eléctrica precipitada del rayo es acompañada por la emisión de luz (el relámpago), causada por el paso de corriente eléctrica que ioniza las moléculas de aire. La electricidad que pasa a través de la atmósfera calienta y expande rápidamente al aire, produciendo el ruido característico del trueno del relámpago.

- **Tormenta solar:** Una tormenta solar es una explosión violenta en la atmósfera del Sol con una energía equivalente a millones de bombas de hidrógeno. Las tormentas solares tienen lugar en la corona y la cromosfera solar, calentando el gas a decenas de millones de grados y acelerando los electrones, protones e iones pesados a velocidades cercanas a la luz. Producen radiación electromagnética en todas las longitudes de onda del espectro, desde señales de radio hasta rayos gamma. Las emisiones de las tormentas solares son peligrosas para los satélites en órbita, misiones espaciales, sistemas de comunicación y la red de suministro.

- **Tornado:** Un tornado es un desastre natural resultado de una tormenta. Los tornados son corrientes violentas de viento que pueden soplar hasta 500 km/h. Pueden aparecer en solitario o en brotes a lo largo de la línea del frente tormentoso.

- **Tsunami:** Un tsunami o Maremoto es una ola gigante de agua que alcanza la orilla con una altura superior a 15 metros. Proviene de las palabras japonesas puerto y ola. Los tsunamis pueden ser causados por terremotos submarinos, o por derrumbamientos.

2. Fuego

Un incendio es una ocurrencia de fuego no controlada que puede abrasar algo que no está destinado a quemarse. Puede afectar a estructuras y a seres vivos. La exposición a un incendio puede producir la muerte, generalmente por inhalación de humo o por desvanecimiento producido por la intoxicación y posteriormente quemaduras graves.

Los incendios se pueden clasifican en cuatro grupos: A, B, C y D.

- Clase A: Incendios que implican madera, tejidos, goma, papel y algunos tipos de plástico.

- Clase B: incendios que implican gasolina, aceites, pintura, gases y líquidos inflamables y lubricantes.

- Clase C: incendios que implican cualquiera de los materiales de la Clases A y B, pero con la introducción de electrodomésticos, cableado o cualquier otro objeto que recibe energía eléctrica, en la vecindad del fuego.

- Clase D: incendios que implican metales combustibles, como el sodio, el magnesio o el potasio u otros que pueden entrar en ignición cuando se reducen a limaduras muy finas.

3. **Fallas de energía.**

   Las fallas, según su naturaleza y gravedad se clasifican en:

   Sobrecarga: Se produce cuando la magnitud de la tensión ("voltaje") o corriente supera el valor preestablecido como normal. Comúnmente estas sobrecargas se originan por exceso de consumos en la instalación eléctrica. Las sobrecargas producen calentamiento excesivo en los conductores de los equipos e incluso llegando a provocar incendios por inflamación.

   Cortocircuito: Se originan por la unión fortuita de dos líneas eléctricas sin aislación, entre las que existe una diferencia de potencial eléctrico. Durante un cortocircuito el valor de la intensidad de corriente se eleva de tal manera, que los conductores eléctricos pueden llegar a fundirse en los puntos de falla, generando excesivo calor, chispas e incluso flamas, con el respectivo riesgo de incendio.

   Falla de aislación: Estas se originan por el envejecimiento de las aislaciones, los cortes de algún conductor, uniones mal aisladas, etc. Estas fallas no siempre originan cortocircuitos, sino en muchas ocasiones se traduce en que superficies metálicas de aparatos eléctricos queden energizadas (con tensiones peligrosas).

   Ausencia de energía: Estas se pueden originar por diversos motivos, sin embargo algunas pueden ser por el envejecimiento de las instalaciones, condiciones del cableado, problemas en el suministro, etc.

4. **Ataques terroristas.**

   En su sentido más amplio, el terrorismo es la táctica de utilizar un acto o una amenaza de violencia contra individuos, grupos o empresas para intentar cambiar el resultado de algún proceso.

5. **Interrupciones organizadas o deliberadas.**

   Las interrupciones se pueden producir por diversas razones, y pueden ser tanto de de Hardware como de Software, sin embargo como su nombre lo indica es una ruptura en el curso normal del funcionamiento de algo. Las interrupciones organizadas generalmente se dan al momento de realizar algún tipo de prueba, o verificación, y al momento de retornar de la interrupción no se cuenta con los recursos requeridos para hacer la restauración.

6. **Sistema y/o fallas de equipo.**

   En este parte se engloba cualquier tipo de error o falla inesperada de algún programa y/o sistema o también algún equipo.

7. **Error humano.**

   Kroll Ontrack (Compañía líder mundial en servicios de recuperación de datos y software de recuperación) ha declarado que los errores humanos son la causa de un número cada vez mayor de solicitudes de recuperación de datos por parte de las empresas.

   Entre los errores humanos más comunes en las empresas, se destacan los siguientes:

   - **Extracción del drive equivocado.** Al intentar sustituir un disco estropeado en un RAID (conjunto redundante de discos independientes), se saca, por equivocación, un disco que está bien.

   - Reformateo de discos. Se reformatea por error el Disco equivocado, cuando se está llevando a cabo una migración de data.

- Restauración con información corrupta o información de backup antigua. Se borra por error un servidor que albergaba una base de datos con información crítica para la empresa, y se restaura mediante un backup anterior con información corrupta o incompleta, antes de que el técnico se dé cuenta de que la copia de backup está dañada.

- Reparación de un RAID dañado. Tras varios fallos en un RAID, se intenta que los discos estropeados vuelvan a estar online y reconstruir la misma configuración, en este proceso, se daña o se corrompe la información contenida en el RAID.

- **Borrado de información.** Se borran sin querer archivos, volúmenes, equipos virtuales o SAN, no existe backup de la información o el backup es antiguo y/o está dañado.

Estos son algunos errores que se pueden dar “por error”, valga la redundancia, sin embargo, puede ser que alguno de estos no necesariamente sea por accidente, más bien que la persona desea producir un daño en la empresa o en algún equipo con algún fin en particular.

8. Virus informáticos.

Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo, propagarse “Infectar” a otras computadoras, cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el procesador valla a ejecutar.

Hoy en día la producción de virus ha aumentado y el Internet colabora enormemente en la dispersión de virus de muchos tipos, incluyendo los "virus caseros". Muchos de estos virus son creados por usuarios inexpertos con pocos conocimientos de programación y, en muchos casos, por simples usuarios que bajan de Internet programas que crean virus genéricos. Ante tantos "desarrolladores" al servicio de la producción de virus la técnica de scanning se ve altamente superada. Las empresas antivirus están constantemente trabajando en la búsqueda y documentación de cada nuevo virus que aparece.

9. Cuestiones legales.

Ante la continua presencia de las amenazas en las organizaciones, se han realizado modificaciones a los contratos de clientes, suplidores, productores, fabricantes, etc. Con el fin de colocar un acápite o clausula que garantice una retribución económica en caso de cualquier interrupción que afecte mis operaciones.

Del mismo modo, los gobiernos han elaborado regulaciones para distintos tipos de organizaciones con el fin de garantizar el mejor desenvolvimiento de las mismas y siguiendo los estándares internacionales o del mercado local.

Si al producirse un desastre en la empresa, se incumple con alguna regulación o acápite contractual, entonces, aparte de involucrarnos en la recuperación del negocio también se verán involucrados en tramites o demandas legales.

10. Conflictos sociales

La confrontación armada de unas naciones contra otras o al interior de una misma nación puede ser una fuente considerable de desastres. De hecho, la Segunda Guerra Mundial es considerada por muchos autores como el mayor

desastre de la era moderna, con sus quince millones de muertos y la vasta destrucción de varias naciones europeas y del Lejano Oriente.

No solo están las guerras, a estos conflictos sociales se le suman otros conflictos a lo externo de la organización como Manifestaciones públicas, explosión social y vandalismo. y dentro de las empresas podemos mencionar los motines, insurrecciones, huelgas, homicidios, dentro de este tipo de desastre se incluyen las intoxicaciones masivas por productos consumo interno.

11. Enfermedades y Epidemias

La enfermedad se convierte en desastre cuando el agente infeccioso adquiere una difusión a nivel de epidemia o pandemia. La enfermedad es el más peligroso de todos los desastres naturales. Entre las diferentes epidemias que ha sufrido la humanidad están la peste negra, la viruela, fiebre porcina (AH1N1) y el SIDA. La vida vegetal y animal también puede ser afectada por las epidemias y pandemias.

2.1.3 Determinación del nivel de vulnerabilidad

Antes de poder indicar que tan vulnerable es Quimidomsa, primero debemos conocer cuáles son sus vulnerabilidades, para esto realizaremos dos análisis:

1- Análisis de seguridad Técnica:

2- Análisis de seguridad Física:

- Análisis de seguridad Técnica: El análisis técnico es la forma en que se obtiene la información específica de como son gestionados, la forma en que son utilizados y manipulados en general los activos de la empresa, buscando identificar vulnerabilidades de seguridad.

<table>
<tr><th colspan="2">Análisis técnico de seguridad</th></tr>
<tr><td colspan="2">Estaciones de trabajo</td></tr>
<tr><td>Son la forma con que estas están configuradas para evitar que los usuarios (con frecuencia de forma inconsciente) permiten la acción de amenazas.

Ejemplos de vulnerabilidades comunes en este tipo
de activos:

- Ausencia de screensaver bloqueado por clave, sin esto las máquinas dejadas solas pueden ser utilizadas por personas no autorizadas.

- Periodicidad de actualización de programas antivirus, forma de organización de los directorios, presencia o ausencia de documentos confidenciales.

- Forma de utilización de la estructura de servidores de ficheros, que garanticen de una manera más eficiente la copia de seguridad de los datos, es decir, su disponibilidad.</td><td>  </td></tr>
<tr><td colspan="2">Servidores</td></tr>
</table>

Los servidores son analizados con prioridades en relación a sus normas de acceso definidas. Se revisan cuáles son los tipos de usuarios que tienen derechos a cuál tipo de información, con base en la clasificación y con relación a la confidencialidad de las informaciones para identificar el exceso o falta de privilegios para la realización de tareas.

El enfoque principal se encuentra en los ficheros de configuración y de definición de usuarios que tienen derechos de administración del ambiente, una vez que son los privilegios de administración los que más amenazan los entornos de tecnología y también son los más anhelados por intrusos.

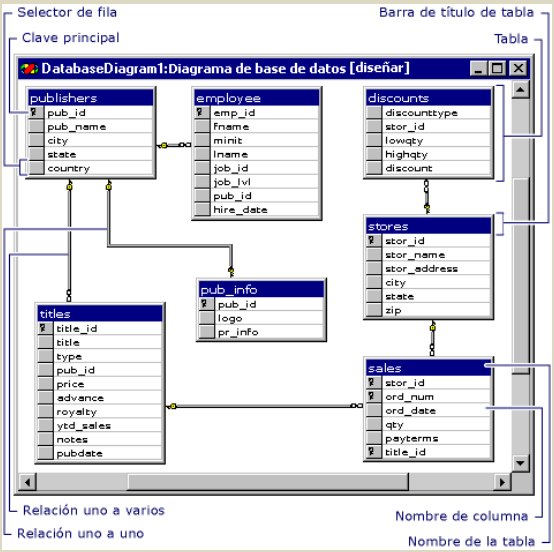
La interacción que estos servidores tienen con las estaciones de trabajo de los usuarios, con las bases de datos y con las aplicaciones que respalda son el objeto del análisis técnico de servidores, independientemente de sus funciones: como ficheros, correo electrónico, FTP, Web y otras.

Equipos de conectividad

El análisis de equipos de conectividad está centrado en la detección de configuraciones que ponen en riesgo las conexiones realizadas por la red de comunicación que respalda un proceso de negocio.

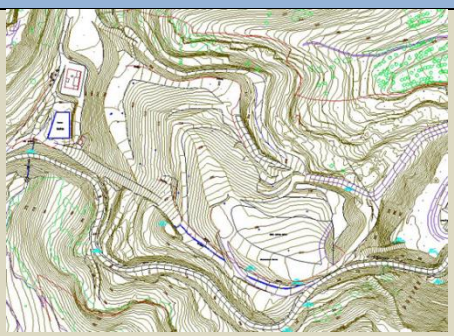
Estos equipos deben poseer un nivel de seguridad muy alto, pues por lo general se sitúan en la entrada de una red de comunicación. Al aplicarse un alto nivel de configuración a estos activos, el acceso externo a la red del proceso de negocio, estará naturalmente más protegido.

Conexiones

Las conexiones de comunicación entre las redes deben estar seguras: fibra óptica, satélite, radio, antenas… Para eso, es importante realizar actividades de análisis sobre la forma con que las conexiones están configuradas y dispuestas en la representación topológica de la red. Esto garantiza que la comunicación sea realizada en un medio seguro, encriptado si fuere necesario, libre de posibilidades de rastreo de paquetes o mensajes, y también como el desvío de tránsito para otros destinos indeseados.	
Bases de datos	
Las bases de datos representan un elemento de importancia extrema en la cadena comunicativa, pues almacenan informaciones relativas a los procesos de negocio y con frecuencia, sobre los usuarios de los procesos de negocio. Son evaluados los niveles de confidencialidad, integridad y disponibilidad de las informaciones que allí están, para que se puedan identificar las necesidades de protección y configuración de seguridad para que la información disponible esté de acuerdo con los principios de la seguridad de la información. En las bases de datos son evaluados los privilegios de los usuarios con relación a los permisos de uso, principalmente en lo que se refiere al acceso de aplicaciones que hacen la lectura y escritura de estas informaciones.	
Aplicaciones	
Las aplicaciones son los elementos que hacen la lectura de las informaciones de un proceso de negocio u organización. De esta manera son un elemento muy crítico, puesto que están haciendo la interfaz entre diversos usuarios y diversos tipos de información con relación a la confidencialidad, integridad y disponibilidad. Se considera, por lo tanto, que las aplicaciones deben garantizar un acceso restrictivo, con base en los privilegios de cada usuario, las informaciones que ellas manipulan, al garantizar que sus configuraciones estén de acuerdo con los principios de seguridad establecidos.	

- Análisis de seguridad Física: Preocupaciones como el exceso de humedad o calor, la disposición de los cables de datos y eléctricos, la existencia de fallas en la organización del entorno, pueden exigir la reestructuración del espacio físico para permitir un área de trabajo que sea segura, y por lo tanto, la información de la organización se encuentre también segura.

Análisis de seguridad Física	
Disposición organizativa	
Se considera la disposición organizativa en especial sobre: - La organización del espacio con relación a cómo están acomodados los muebles y los activos de información. - Que las áreas de circulación de personas en lugares de alto transito estén libres de activos de valor o importancia. - Que los activos de alta importancia se ubiquen en áreas libres de acceso de personas que no están autorizadas para operarlos.	
Sistemas de combate a incendio	
Se considera la disposición de los mecanismos de combate a incendio, cuidando que estén en los lugares adecuados: - Los detectores de humo. - Los aspersores de agua - Los extintores de incendio (Sin importar el tipo de sistemas que se esté utilizando) - Entre otras cosas.	
Control de acceso	

Se ocupa de la disposición de sistemas de detección y autorización de acceso a las de personas, para esto se hace uso de: - Cámaras de video, - Personal de seguridad, - Ingreso a las instalaciones por control de acceso, - Mecanismos de reconocimiento individual, - entre otros.	
Exposición a clima y medio ambiente	
Disposición de las ventanas y puertas de áreas críticas. Se preocupa que se encuentren ubicadas próximas a activos críticos, Si los activos críticos reciben luz solar o posibilidad de amenaza causadas por los fenómenos de la naturaleza, como viento o lluvias fuertes.	
Topografía	
Se interesa en la localización del data center, de la sala de cómputo, del sitio de servidores, o cualquier área crítica con relación a la topografía del terreno si se encuentran en el subsuelo, al alcance de inundaciones, próximas a áreas de riesgo como proximidad al mar, ríos o arroyos o áreas de retención de agua o con posibilidad de pérdidas de cañerías hidráulicas.	

Luego de haber analizado todos los aspectos de seguridad física y ambiental, conocer los control de autenticación, autorización, comunicación y acceso, así como los parámetros de las auditorias, y políticas de antivirus, y backup, Podemos indicar las siguientes debilidades en el Área de TI:

- Control de accesos:

La clave de los sistemas transaccionales no expira, la única clave que hace esta operación es la clave del sistema operativo, debería de expirar con frecuencia regular.

- Seguridad en la red de área local (LAN)
  - Los cables del suministro eléctrico se encuentra ligados con el cableado de la red. Al momento del diseño del datacenter no contemplaron una entrada independiente para cada tipo de cableado.

- Seguridad especifica en los servidores

Del mismo modo que en los sistemas transaccionales es requerido que las claves de acceso para cada uno de los servidores sea expirada con una frecuencia regular y aplicar algún tipo de parámetro para el control de dicha clave.

- Otros aspectos en los que hacemos hincapiés es en la posibilidad de ocurrencias de incendios en la planta de producción, ya que en la planta se trabaja con químicos que en caso de presentarse algún error humano de la parte operativa puede provocar un incendio.

A continuación presentamos una tabla de riesgo priorizado donde veremos aquellos incidentes de los cuales deben cuidarse y cuales vulnerabilidades de las expuestas anteriormente pueden atacar a la empresa Quimidomsa.

Matriz de riesgo priorizado.

Activos	Amenazas	Vulnerabilidad	Impacto a la organización	Nivel de Impacto	Probabilidad de ocurrencia	Medición del riesgo	Prioridad
Infraestructura, inmobiliario y materia prima	Huracán	Ventanas de cristal en el frente y laterales	Perdida de Recursos Humanos	5	4	17	E
			Daños a la estructura física	5			
			Perdida de materia prima	4			
			Daños al Inmobiliario	3			
		Arboles alrededor de las instalaciones	Perdida de Recursos Humanos	5		19	E
			Falla Eléctrica	5			
			Perdida de Conectividad (Internet/Teléfono)	5			
			Daños a la estructura física	5			
			Perdida de materia prima	4			
	Inundaciones	Agua en exceso dentro de la localidad.	Perdida de Recursos Humanos	5	2	9	M
			Falla Eléctrica	5			
			Daños a la estructura física	5			
			Perdida de materia prima	4			
			Daños al Inmobiliario	3			
		Data center ubicado en el primer piso	Daños de Equipos	5		10	A
			Perdida de Información	5			
	Sismos	Diseño del edificio no es antisismico	Perdida de Recursos Humanos	5	2	9	M
			Interrupción del sistema	4			
			Daños de Equipos	5			
			Perdida de Información	5			
			Daños a la estructura física	5			
			Perdida de materia prima	4			
			Daños al Inmobiliario	3			
		Cableado eléctrico ligado al cableado de la red	Perdida de Conectividad (Internet/Teléfono)	5		10	A
			Falla Eléctrica	5			

Nivel de impacto (1 Mínimo - 5 Catastrófico) **Probabilidad de ocurrencia (1 Raro - 5 Casi Seguro)**

Prioridad (B-Baja, M-Moderada, A-Alta, E-Extrema)

Matriz de riesgo priorizado 2.

Activos	Amenazas	Vulnerabilidad	Impacto a la organización	Nivel de Impacto	Probabilidad de ocurrencia	Medición del riesgo	Prioridad
Infraestructura, inmobiliario y materia prima	Incendios	Accidentes en la planta de producción	Perdida de Recursos Humanos	5	4	18	E
			Interrupción del sistema	4			
			Daños de Equipos	5			
			Perdida de Información	5			
			Daños a la estructura física	5			
			Perdida de materia prima	4			
			Daños al Inmobiliario	3			
		Cableado eléctrico ligado al cableado de la red	Perdida de Conectividad (Internet/Teléfono)	5		20	E
			Falla Eléctrica	5			
	Vandalismo	Huelgas o conflictos sociales en las cercanías de las instalaciones	Perdida de Recursos Humanos	5	3	14	A
			Daños de Equipos	5			
			Perdida de Información	5			
			Daños a la estructura física	5			
			Perdida de materia prima	4			
			Daños al Inmobiliario	3			
	Conflictos Bélicos (Guerras, Terrorismo)	Incidentes que impacten República Dominicana y/o Guatemala.	Perdida de Recursos Humanos	5	1	5	B
			Daños de Equipos	5			
			Perdida de Información	5			
			Daños a la estructura física	5			
			Perdida de materia prima	4			
			Daños al Inmobiliario	3			
			Perdida de Conectividad (Internet/Teléfono)	5			

Nivel de impacto (1 Mínimo - 5 Catastrófico) **Probabilidad de ocurrencia (1 Raro - 5 Casi Seguro)**

Prioridad (B-Baja, M-Moderada, A-Alta, E-Extrema)

Matriz de riesgo priorizado 3.

Activos	Amenazas	Vulnerabilidad	Impacto a la organización	Nivel de Impacto	Probabilidad de ocurrencia	Medición del riesgo	Prioridad
Sistemas	Virus	Desactualización o expiración de Antivirus	Perdida de Información	5	3	14	A
			Daños de Equipos	5			
			Fallas en los procesos	4			
		Malas Políticas de control de acceso	Perdida de Información	5		14	A
			Daños de Equipos	5			
			Fallas en los procesos	4			
		Dispositivos portables conectados sin autorización	Perdida de Información	5		14	A
			Daños de Equipos	5			
			Fallas en los procesos	4			
		Equipos de visitantes conectados a la red sin inspección	Perdida de Información	5		14	A
			Daños de Equipos	5			
			Fallas en los procesos	4			
	Hackers	Malas Políticas de control de acceso a la Red	Perdida de Información	5	5	23	E
			Daños de Equipos	5			
			Fallas en los procesos	4			
		Vulnerabilidad de Contraseñas	Perdida de Información	5		23	E
			Daños de Equipos	5			
			Fallas en los procesos	4			
	Errores Humano	Malas Políticas de control de acceso	Perdida de Información	5	3	12	A
			Datos erróneos	3			
		Manejo inadecuado de equipo	Perdida de Información	5		14	A
			Daños de Equipos	5			
			Fallas en los procesos	4			
		Equivocaciones o descuidos	Daños de Equipos	5		14	A
			Perdida de Información	5			
			Fallas en los procesos	4			

Nivel de impacto (1 Mínimo - 5 Catastrófico) **Probabilidad de ocurrencia (1 Raro - 5 Casi Seguro)**

Prioridad (B-Baja, M-Moderada, A-Alta, E-Extrema)

Matriz de riesgo priorizado 4.

Activos	Amenazas	Vulnerabilidad	Impacto a la organización	Nivel de Impacto	Probabilidad de ocurrencia	Medición del riesgo	Prioridad
Sistemas	Ingeniería Social	Malas Políticas de control de acceso a la Red	Perdida de Información	5	4	19	E
			Daños de Equipos	5			
			Fallas en los procesos	4			
		Vulnerabilidad de Contraseñas	Perdida de Información	5		19	E
			Daños de Equipos	5			
			Fallas en los procesos	4			
Nivel de impacto (1 Mínimo - 5 Catastrófico)					Probabilidad de ocurrencia (1 Raro - 5 Casi Seguro)		
Prioridad (B-Baja, M-Moderada, A-Alta, E-Extrema)							

Escala de prioridad:

			Impacto				
			Mínimo 1	Menor 2	Moderado 3	Mayor 4	Catastrófico 5
Probabilidad	Raro	1	Bajo	Bajo	Moderado	Alto	Alto
	Improbable	2	Bajo	Bajo	Moderado	Alto	Extremo
	Posible	3	Bajo	Moderado	Alto	Extremo	Extremo
	Muy probable	4	Moderado	Alto	Alto	Extremo	Extremo
	Casi Seguro	5	Alto	Alto	Extremo	Extremo	Extremo

Los riesgos Extremos: Deben ponerse en conocimiento de los directores y más altas esferas de la empresa y aplicarse un seguimiento continuo.

Los riesgos Altos: Requieren la atención de los directores

Los riesgos Moderados: Deben ser objeto de seguimiento adecuado por parte de los niveles medios de dirección

Los riesgos Bajos: Deben ser objeto de seguimiento por parte de los supervisores.

2.1.4 Identificación de controles existentes

Por la naturaleza de la empresa Quimidomsa, son requeridos estrictos controles de protección ambiental y de seguridad física, cumpliendo así con las normas y regulaciones establecidas por el estado Dominicano y el Guatemalteco. En el ámbito de seguridad en el área de tecnología de información hacemos un resumen de sus principales políticas de seguridad:

1. La confidencialidad de toda la información debe ser mantenida a través de un discreto y obligatorio control de acceso.
2. Internet y el acceso a otros servicios externos están restringidos, solamente el personal autorizado tendrá acceso.
3. El acceso para la información en todas las laptop debe ser asegurado con encriptación o por otro medio, para proveer confidencialidad de la data en caso de pérdida o robo del equipo.
4. Solo el software autorizado y licenciado puede ser instalado, Y la instalación debe de realizarse por el personal del Departamento de Tecnologías.
5. El uso de software sin autorización está prohibido. En caso de que software sin autorización sea descubierto, este será removido de la estación de trabajo inmediatamente.
6. La información solo puede ser transferida por los propósitos determinados en la política organizacional de protección de data.
7. Todos los diskettes y los medios removibles de Fuentes externas deben ser revisadas por un antivirus antes de ser utilizadas en la organización.
8. La clave de Windows debe de consistir en una mezcla de al menos 8 caracteres, debe ser cambiada cada 40 Días y debe ser única.
9. Las configuraciones de las estaciones de trabajo, deben ser cambiadas solo por el Personal del Departamento de Tecnologías.

10. Para prevenir la perdida de disponibilidad de recursos de TI, medidas deben ser tomadas para el backup de la data, aplicaciones y la configuración de todas las estaciones de trabajo.

Ver en el apéndice II el listado completo de las políticas de seguridad para el área de TI vigentes en Quimidomsa.

2.1.5 Controles sugeridos

Para cada una de las vulnerabilidades expuestas sugerimos la aplicación de controles específicos, con los cuales se lograrían minimizar.

Control de accesos a sistemas y a servidores

Sugerimos que se aplique como política que las claves de acceso a los sistemas y servidores sea expirada cada 40 días y que estás no puedan ser reutilizadas, es decir no puede ser igual a las últimas claves (Como parámetro recomendamos utilizar las últimas 10 claves). La clave nueva deberá contener por lo menos un carácter en mayúscula y un número.

Adicional a esto sugerimos que en todas las claves de acceso se les permita un intento máximo de 3 oportunidades, luego de esto la clave será bloqueada, y para hacer el desbloqueo solo se autorizará al personal de Tecnología.

Reinstalación de cableado eléctrico área del datacenter.

En relación al cableado del suministro eléctrico, sugerimos realizar una reinstalación del cableado eléctrico en el área del datacenter, con esto garantizamos una ruta de acceso y organización independiente para cada configuración de cables (Electricidad y red).

Sugerimos que esta reinstalación del cableado sea realizada en 1 día abarcando este desde un Sábado en la tarde hasta concluir un Domingo en la Tarde, con esto cubrimos

cualquier improvisto que se pueda presentar desde la terminación del trabajo hasta el reinicio de operaciones el Lunes siguiente.

Es importante mantener una adecuada estructura de cableados ya que nos permite mayor rapidez y eficiencia al momento de detectar algún inconveniente de cableado, si todos están ligados puede que el proceso tan solo de identificar donde está el fallo se vuelva complicado. Adicionalmente cabe mencionar que el cableado debe tener un criterio de colación y este debe ser plasmado en un diagrama de cableados que es necesario durante el proceso de recuperación de la organización.

Alta disponibilidad de almacenamiento.

Para lograr una alta disponibilidad en el almacenamiento y evitar las vulnerabilidades de pérdida de información proponemos la implementación de un NAS. Un dispositivo de almacenamiento conectado a la red (Network-Attached Storage - NAS) es un servidor destinado exclusivamente al almacenamiento de datos (es decir, un array de almacenamiento) que se conecta a la red. Los clientes envían las peticiones de archivos directamente al dispositivo NAS, evitando cargar a los servidores destinados a fines generales de la red.

Los dispositivos NAS poseen un sistema de archivos capaz de suministrar archivos de distintas plataformas, ya que son capaces de leer los datos de los principales sistemas de archivos.

Los dispositivos NAS también poseen la capacidad de compartir una copia de los datos entre varios servidores de aplicaciones, lo que los convierte en una magnífica herramienta de colaboración entre plataformas. Además, son más económicos que los servidores estándar. De hecho, la relación costo/rendimiento de este tipo de dispositivos los convierte en un producto muy atractivo.

Tabla de riesgo residual

En esta tabla aplicaremos los controles a cada una de las vulnerabilidades con el objetivo de eliminar o minimizar el impacto en Quimidomsa. El riesgo resultante serán los puntos en los que más debo enfocarme en el plan de recuperación.

Amenazas	Vulnerabilidad	Probabilidad de ocurrencia	Prioridad	Controles Aplicados	Efectividad del control	Riesgo residual	Riesgo general
Sismos	Cableado eléctrico ligado al cableado de la	2	**A**	Reinstalación de cableado eléctrico	5	5	**B**
Vandalismo	Huelgas o conflictos sociales en las cercanías de las	3	**A**	Precaución y prevención	3	11	**A**
Virus	Desactualización o expiración de Antivirus	3	**A**	Actualización constante por parte de TI	5	9	**M**
	Malas Políticas de control de acceso		**A**	Robustecer las políticas de control de accesos	5	9	**M**
	Dispositivos portables conectados sin		**A**	Eliminar el acceso según perfil de usuario	5	9	**M**
	Equipos de visitantes conectados a la red sin inspección		**A**	Verificación y registro de los equipos de visitantes	5	9	**M**
Errores Humano	Malas Políticas de control de acceso	3	**A**	Robustecer las políticas de control de accesos	5	7	**M**
	Equivocaciones o descuidos		**A**	Precaución y concientización	3	11	**A**
	Manejo inadecuado de equipo		**A**	Precaución y concientización	3	11	**A**
Inundaciones	Data center ubicado en el primer piso	2	**A**	Precaución y prevención	3	7	**M**
Probabilidad de ocurrencia (1 Raro - 5 Casi Seguro)				**Efectividad del control (1 Poco efectivo - 5 Bastante efectivo)**			
Prioridad (B-Baja, M-Moderada, A-Alta, E-Extrema)				**Riesgo Residual (B-Baja, M-Moderada, A-Alta, E-Extrema)**			

Tabla de riesgo residual (continuación)

Amenazas	Vulnerabilidad	Probabilidad de ocurrencia	Prioridad	Controles Aplicados	Efectividad del control	Riesgo residual	Riesgo general
Huracán	Ventanas de cristal en el frente y laterales	4	E	Proteger las ventanas ante alerta de huracán	3	15	A
	Arboles alrededor de las instalaciones	4	E	Cortar o Talar aquellos que sean amenazas	3	15	A
Incendios	Accidentes en la planta de producción	4	E	Precaución, prevención y capacitación	3	15	A
	Cableado eléctrico ligado al cableado de la		E	Reinstalación de cableado eléctrico	5	15	A
Hackers	Malas Políticas de control de acceso a la	5	E	Robustecer las políticas de control de accesos	5	18	E
	Vulnerabilidad de Contraseñas		E			18	E
Ingeniería Social	Malas Políticas de control de acceso a la	4	E	Robustecer las políticas de control de accesos	5	14	A
	Vulnerabilidad de Contraseñas		E			14	A
Probabilidad de ocurrencia (1 Raro - 5 Casi Seguro)				**Efectividad del control (1 Poco efectivo - 5 Bastante efectivo)**			
Prioridad (B-Baja, M-Moderada, A-Alta, E-Extrema)				**Riesgo Residual (B-Baja, M-Moderada, A-Alta, E-Extrema)**			

Al aplicar los controles necesarios logramos reducir lo siguiente:

- Minimizar los riesgos “Extremo” en un 75% llevándolos a “Alto”.
- El 60% de los riesgos “Alto” fueron llevados a “moderado” y un 10% fue descendido al mínimo nivel de riesgo.

2.2 Activos del área de Tecnología de información

Para iniciar el proyecto, debemos tomar en cuenta todos los recursos que actualmente existen en la empresa Quimidomsa para desarrollar un buen plan de recuperación de Desastres (DRP).

A continuación les presentamos un inventario de los activos del área de tecnología y su ubicación:

Hardware

Equipo	Nombre	Marca	Modelo	Ubicación
DES & QAS SAP Server	QMDDEV	Compaq	ProLiant ML530 G2	Sede Rep. Dom.
Appl. Server SAP	QMDPRD	Compaq	ProLiant DL580 G2	Sede Rep. Dom.
File Server Dominicana	QMDRPS	Dell	PowerEdge 400SC	Sede Rep. Dom.
Servidor Cámaras de Seg.	QMDSCAM	Dell	PowerEdge R300	Sede Rep. Dom.
Domain Controller	QMDSDC	Dell	PowerEdge R300	Sede Rep. Dom.
Isa Server	QMDISA	Dell	PowerEdge 400SC	Sede Rep. Dom.
File Server Guatemala	QMGTFILE	Dell	PowerEdge R300	Sede Guatemala
Servidor de AntiVirus	QMDSAV	Dell	PowerEdge R300	Sede Rep. Dom.
Servidor App. Retail.	QMDSAPP	Dell	PowerEdge R300	Sede Rep. Dom.
Servidor de RRHH	QMDRRHH	Compaq	ProLiant DL360 G2	Sede Rep. Dom.
Exchange Server	QMDMAIL	Dell	PowerEdge R300	Sede Rep. Dom.
servidor de Virtualizacion	QMDNCOM	Dell	PowerEdge R300	Sede Rep. Dom.
servidor de Virtualizacion	QMDNCOM2	Dell	PowerEdge R300	Sede Rep. Dom.
Servidor de RRHH GT	QMGTRRHH	Dell	PowerEdge R300	Sede Guatemala
Servidor VOIP	QMVOIP	Dell	PowerEdge R300	Sede Rep. Dom.

Software

Software	Nombre	Proveedor	Ubicación
SAP Mandante Desarrollo	SAP ERP 5	SAP	QMDDEV
SAP Mandante Calidad	SAP ERP 5	SAP	QMDDEV
SAP Mandante Productivo	SAP ERP 5	SAP	QMDPRD
Grabación de cámaras Seg.	NVR v2.1.30	NVR	QMDSCAM
Gestión y acceso RED	ISA Server 2006	Microsoft	QMDISA
AntiVirus & AntiSpam	Symantec Antivirus	Symantec	QMDSAV
Punto de venta	Retail PRO	RIS	QMRPS
Gestión de RRHH & Nomina	Eikon	Eikon	QMDRRHH
Gestión de E-mails	Exchange	Microsoft	QMDMail
Virtual Machine	Virtual Machine	VMware, Inc.	QMDNCOM 1 y 2
Gestión de acceso Puertas	Intelli-M Supervisor Plus	Intelli-M	QMDNCOM
Punto de venta	SAP POS	SAP	QMDSAPP
Mesa de Ayuda	SYSAID	SYSAID	QMDNCOM
Voz sobre IP	Asterick	Asterick	QMDVOIP

Sistema Operativo

Sistema Operativo	Cantidad	Release	Proveedor
Windows Server 2003 "R2" Enterprise Edition	2	SP2	Windows
Windows Server 2003 Standard Edition	10	SP2	Windows
VMware	2	ESX Server	EMC
Linux RedHat	1	Versión 9	RED HAT

Motor Base de datos

Base de datos	Cantidad	Versión	Release	Fabricante
Microsoft SQL Server Enterprise Edition	2	2000	SP4	Microsoft
Microsoft SQL Server Standard Edition	4	2005	SP2	Microsoft

Tasación de activos

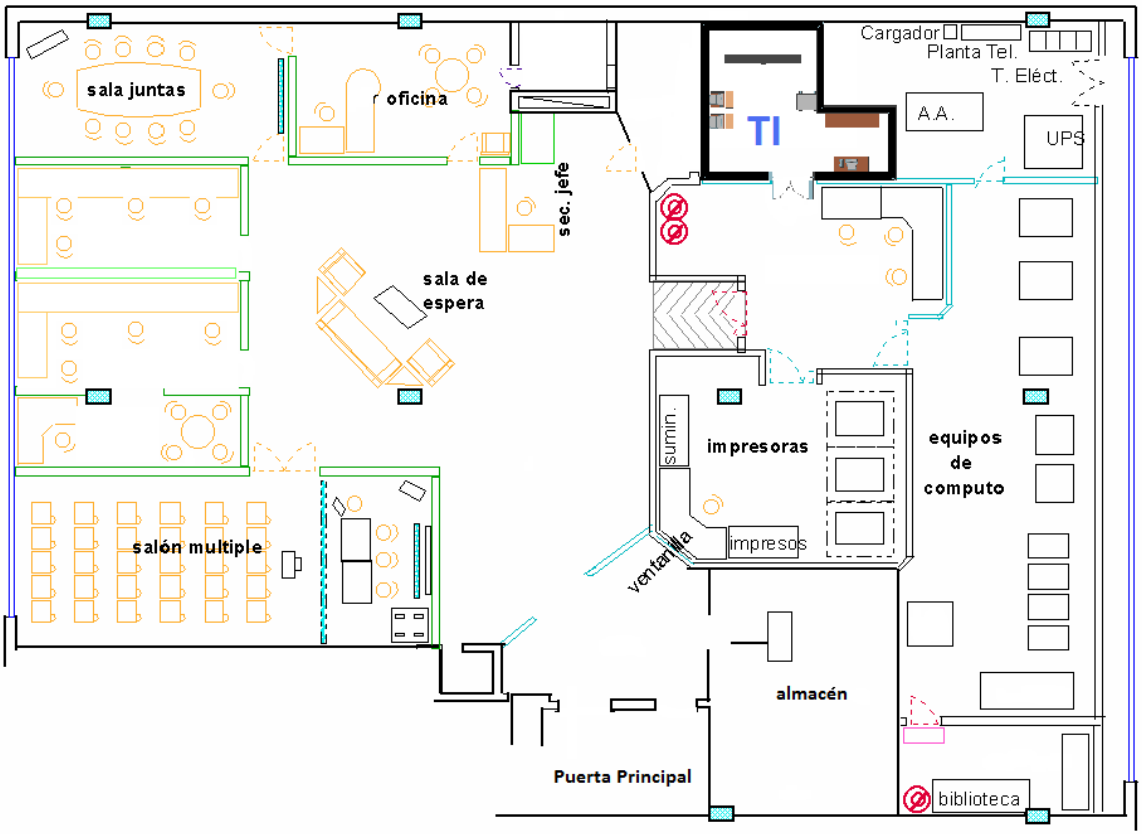
La tasación de los activos es un instrumento para obtener efecto que pueda recibir la empresa con la perdida de algún activo. Se utilizara como medición la confidencialidad, integridad y disponibilidad.

Activo	Confidencialidad	Integridad	Disponibilidad	Total
DES & QAS SAP Server	3	4	3	10
Appl. Server SAP	5	5	5	15
File Server Dominicana	3	3	2	8
Servidor Cámaras de Seg.	2	2	1	5
Domain Controller	4	5	5	14
ISA Server	3	3	3	9
File Server Guatemala	3	3	3	9
Servidor de AntiVirus	2	3	3	8
Servidor App. Retail.	2	2	1	5
Servidor de RRHH	4	3	4	11
Exchange Server	5	4	5	14
servidor de Virtualizacion I	3	4	4	11
servidor de Virtualizacion II	3	4	4	11
Servidor de RRHH GT	4	3	4	11
Servidor VOIP	4	4	5	13

1 = Muy poco, 5= Muy Alto

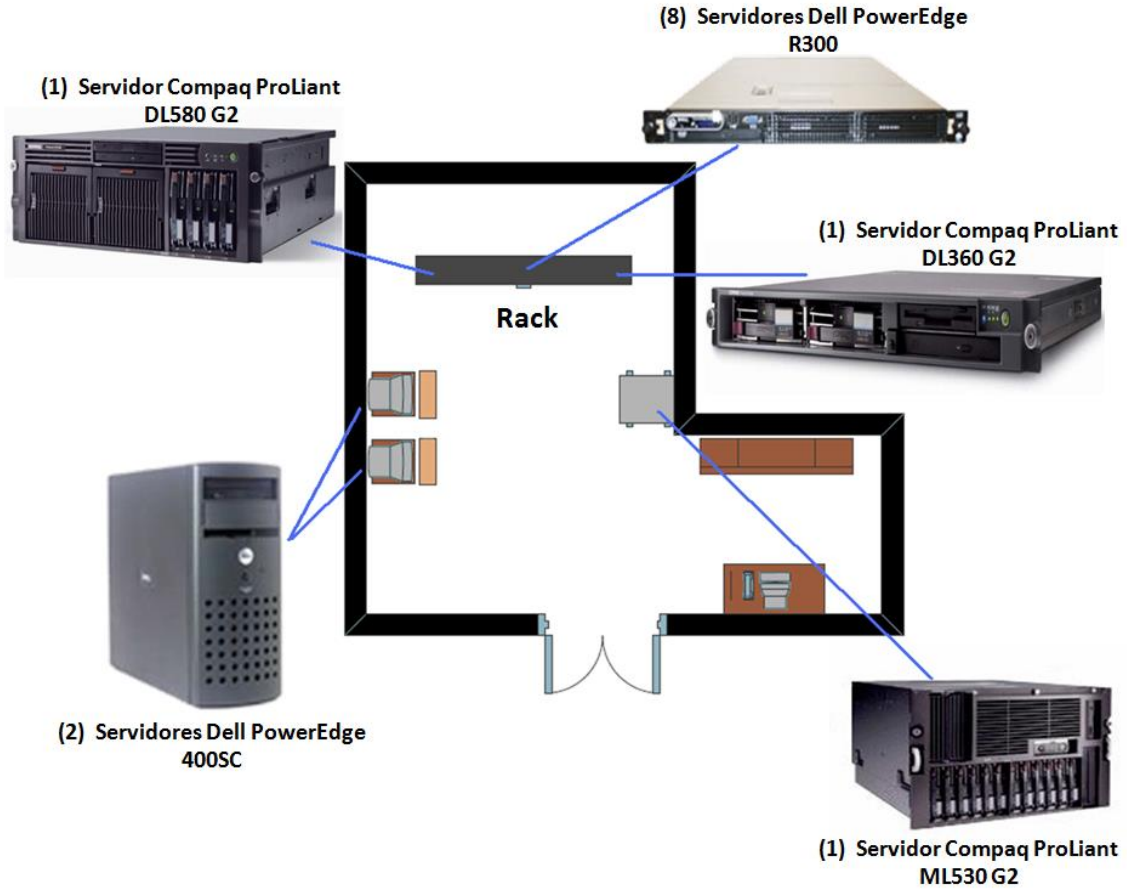
2.2.1 Ubicación área de Tecnología de Información

El área de tecnología de información de la empresa Quimidomsa es un centro relativamente pequeño. A continuación se muestra el plano de la ubicación física de está área, la zona indicada como “Equipos de computo” es la zona destinada a los operadores denominada. El área del datacenter está indicada como “TI” en color azul.



Detalle de componentes en el área de TI

En la siguiente imagen se muestra la disposición, cantidad y configuración de los equipos dentro del área de TI.



2.3 Análisis de impacto al negocios (BIA)

Objetivo

El propósito fundamental del Análisis de Impacto sobre el negocio, conocido más comúnmente como BIA, (Business Impact Analisys) es determinar y entender qué procesos de la empresa Quimidomsa es esencial para la continuidad de las operaciones y calcular su posible impacto. Además, permite identificar las áreas que sufrirán las pérdidas financieras y operacionales, estimando el tiempo de recuperación de algún desastre.

Teniendo el conocimiento del impacto al negocio, se pueden dimensionar los controles de prevención y recuperación, de acuerdo a las necesidades de Quimidomsa, evitando la sobre inversión o la sub inversión.

Para obtener esta información, realizamos entrevistas a todo el personal responsable de los procesos de negocios de la empresa. (ver Apéndice III - Cuestionario BIA).

2.3.1 Identificación procesos y recursos.

En este proyecto se consideran los siguientes departamentos para el análisis de impacto del negocio:

1. Ventas.
2. Logística.
3. Compras.
4. Producción.
5. Finanzas.
6. Recursos Humanos.
7. Tecnología de Información.

A continuación describiremos todos los procesos críticos de cada departamento señalado anteriormente:

1. Ventas

Procesos

Para el propósito de este informe, fueron tomado en cuenta los procesos de ventas locales, exportaciones, servicios y servicio al cliente, donde se consideran parte de la función de ventas.

#	Proceso de Negocio	Descripción	Herramientas TI
1	Ventas Locales	Es el proceso en el cual se realiza acuerdos de ventas con clientes locales.	SAP
2	Ventas Exportación	Es el proceso en el cual se realiza acuerdos de ventas con clientes extranjeros, donde se consideran otros recursos externos (aduanas, transporte, etc).	SAP
3	Ventas de Servicios	Es el proceso en el cual se realiza ventas de servicios tales como energía eléctrica y vapor que se generan en las instalaciones de Quimidomsa.	SAP
4	Re-ventas	Es el proceso en el cual se realiza acuerdos de ventas con productos importados.	SAP
5	Servicio al Cliente	Es el proceso en el cual brinda el soporte a los clientes existentes.	SAP

Impacto Operacional

El impacto operacional será medido en la escala de 0 al 4 donde 0 = Muy bajo y 4 = Muy Alto. El valor de impacto de cada operación indica cuan severo seria el impacto a la compañía.

Operación	Valor
Flujo de Caja	4
Ventaja Competitiva	3
Confianza del cliente	3
Reportes financieros	2
Imagen del negocio	2
Moral del Empleado	3
Servicio al Cliente	3
Comisiones	1
Proveedores	1
Entidades Regulatorias	0
Otros	0

Reportes regulatorios

#	Unidad de negocio	Reporte	Descripción	Pais	Frecuencia	Entidad
1	Ventas	6-07	Ventas de Bienes y/o Servicios	República Dominicana	Anual	DGII
2	Ventas	LVGT	Libro de ventas	Guatemala	Mensual	SAT

Numero del personal de recuperación requerido

El número del personal de recuperación por día, representa el número del personal interno requerido para esta unidad de negocios.

Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7	Día 14	Día 21	Día 28
3	3	3	3	3	3	5	5	5	5

MTO, RPO y RTO para Ventas

#	Procesos Críticos	Tiempo Máximo de Tolerancia (MTO)	Objetico de Punto de Recuperación (RPO)	Objetico de Tiempo de Recuperación (RTO)
1	Ventas Locales	2 Días	1 Días	0.5 Días
2	Ventas Exportación	2 Días	1 Días	0.5 Días
3	Ventas de Servicios	3 Días	2 Días	1 Días

2. Logística

Procesos

Para el propósito de este informe, fueron tomados en cuenta los procesos de Despacho y distribuccion, Entrada y salida de mercancías y Gestión de aduanas, donde se consideran parte de la función de logistica.

#	Proceso de Negocio	Descripción	Herramientas TI
1	Despacho	Es el proceso en el cual se realiza y se gestiona las salidas de mercancías.	SAP, Exchange
2	Inventario	Es el proceso en el cual se realiza un conteo de las mercancías de almacén y se compara con el sistema.	SAP, Excel
3	Distribución	Es el proceso en el cual se coordina todo el transporte local y de exportación de las mercancías.	Excel, Software inhouse
4	Abastecimiento	Es el proceso en el cual se realiza y se gestiona las entradas de mercancías.	SAP
5	Aduana	Es el proceso en el cual se realiza la aduanalización de todas mercancías de importación como exportación	SAP

Reportes regulatorios

#	Unidad de negocio	Reporte	Descripción	Pais	Frecuencia	Entidad
1	Logística	DUA	Declaración de Aduana	República Dominicana	diario	DGA
2	Logística	DUA	Declaración de Aduana	Guatemala	diario	SAT

Impacto Operacional

El impacto operacional será medido en la escala de 0 al 4 donde 0 = Muy bajo y 4 = Muy Alto. El valor de impacto de cada operación indica cuan severo seria el impacto a la compañía.

Operación	Valor
Flujo de Caja	3
Ventaja Competitiva	2
Confianza del cliente	2
Reportes financieros	0
Imagen del negocio	2
Moral del Empleado	1
Servicio al Cliente	3
Comisiones	0
Proveedores	1
Entidades Regulatorias	0
Otros	0

Numero del personal de recuperación requerido

El número del personal de recuperación por día, representa el número del personal interno requerido para esta unidad de negocios.

Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7	Día 14	Día 21	Día 28
0	0	0	0	0	0	0	0	0	0

MTO, RPO y RTO para Ventas

#	Procesos Críticos	Tiempo Máximo de Tolerancia (MTO)	Objetico de Punto de Recuperación (RPO)	Objetico de Tiempo de Recuperación (RTO)
1	Despacho	2 Días	1 Días	0.7 Días
2	Inventario	4 Días	3 Días	2 Días
3	Distribución	4 Días	2 Días	1 Días
4	Abastecimiento	4 Días	3 Días	2 Días
5	Aduana	4 Días	3 Días	2 Días

3. Compras

Procesos

Para el propósito de este informe, fueron tomados en cuenta los procesos de compras locales e internacionales, donde se consideran parte de la función de compras.

#	Proceso de Negocio	Descripción	Herramientas
1	Negociación y compra locales de bienes y servicios	Negociación con los vendedores y colocar ordenes de bienes y servicios de proveedores locales	SAP, Exchange
2	Mantenimiento con Contratos de servicios	Es el proceso en el cual se gestiona y se actualiza todos los contratos de servicios utilizados en la empresa	SAP, Exchange
3	Negociación y compras internacionales de bienes y servicios	Negociación con los vendedores y colocar ordenes de bienes y servicios de proveedores Internacionales	SAP, Exchange
4	Gestión de solicitudes de pedidos	Es el proceso en el cual se gestiona y se convierte a pedido las solicitudes de pedido hechas por el personal.	SAP, Exchange

Reportes regulatorios

#	Unidad de negocio	Reporte	Descripción	Pais	Frecuencia	Entidad
1	Compras	707	Reporte compras de bienes y servicios	RD	Mensual	DGII
2	Compras	LCGT	Libro de compras	GT	Mensual	SAT

Impacto Operacional

El impacto operacional será medido en la escala de 0 al 4 donde 0 = Muy bajo y 4 = Muy Alto. El valor de impacto de cada operación indica cuan severo seria el impacto a la compañía.

Operación	Valor
Flujo de Caja	3
Ventaja Competitiva	3
Confianza del cliente	1
Reportes financieros	2
Imagen del negocio	2
Moral del Empleado	1
Servicio al Cliente	1
Comisiones	0
Proveedores	4
Entidades Regulatorias	4
Otros	0

Numero del personal de recuperación requerido

El número del personal de recuperación por día, representa el número del personal interno requerido para esta unidad de negocios.

Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7	Día 14	Día 21	Día 28
5	5	5	5	5	5	5	5	5	5

MTO, RPO y RTO para Ventas

#	Procesos Críticos	Tiempo Máximo de Tolerancia (MTO)	Objetico de Punto de Recuperación (RPO)	Objetico de Tiempo de Recuperación (RTO)
1	Negociación y compra locales de bienes y servicios	4 Días	3 Días	2 Días
2	Mantenimiento con Contratos de servicios	5 Días	3 Días	2 Días
3	Negociación y compras internacionales de bienes y servicios	4 Días	2 Días	1 Días
4	Gestión de solicitudes de pedidos	4 Días	3 Días	2 Días

4. Producción

Procesos

Para el propósito de este informe, fueron tomados en cuenta los procesos producción y planificación, además de gestión de calidad, donde se consideran parte de la función de Producción.

#	Proceso de Negocio	Descripción	Herramientas
1	Gestión de Ordenes de Procesos	Es el proceso mediante el cual se crean las órdenes de proceso, listado de herramientas y listado de recursos a utilizar para Producción.	SAP
2	Planificación de la Producción	Es el proceso en el cual se Planifica todas la producción a realizar.	SAP, Excel
3	Gestión de Calidad	Es el proceso en el cual se garantiza la calidad de los productos realizados.	Papel

Reportes regulatorios

#	Unidad de negocio	Reporte	Descripción	País	Frecuencia	Entidad
1	Producción	N/A	No Requerido.	RD	N/A	N/A
2	Producción	N/a	No Requerido.	GT	N/A	N/A

Impacto Operacional

El impacto operacional será medido en la escala de 0 al 4 donde 0 = Muy bajo y 4 = Muy Alto. El valor de impacto de cada operación indica cuan severo seria el impacto a la compañía.

Operación	Valor
Flujo de Caja	4
Ventaja Competitiva	3
Confianza del cliente	3
Reportes financieros	3
Imagen del negocio	4
Moral del Empleado	3
Servicio al Cliente	4
Comisiones	2
Proveedores	1
Entidades Regulatorias	0
Otros	0

Numero del personal de recuperación requerido

El número del personal de recuperación por día, representa el número del personal interno requerido para esta unidad de negocios.

Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7	Día 14	Día 21	Día 28
12	12	12	12	12	12	12	12	12	12

MTO, RPO y RTO para Ventas

#	Procesos Críticos	Tiempo Máximo de Tolerancia (MTO)	Objetico de Punto de Recuperación (RPO)	Objetico de Tiempo de Recuperación (RTO)
1	Gestión de Ordenes de Procesos	3 Días	2 Días	0.7 Días
2	Planificación de la Producción	4 Días	2 Días	1 Días
3	Gestión de Calidad	4 Días	3 Días	2 Días

5. Finanzas

Procesos

Para el propósito de este informe, Cuentas por pagar, Cuentas por cobrar, Contralor, Presupuesto, Caja Chica, entre otros fueron considera parte de la función financiera.

#	Proceso de Negocio	Descripción	Herramientas
1	Presupuesto	En este proceso se analiza las variantes entre lo planeado y los resultados actuales	SAP, Excel
2	Cuentas Por Cobrar	Es el proceso en el cual se gestiona los cobros de facturas a crédito con el propósito que se cumplan los pagos dentro del plazo establecido en el acuerdo de venta.	SAP
3	Tesorería	Es el proceso de planeación y el manejo de los fondos de la empresa en el corto, mediano y largo plazo.	SAP, Quicken
4	Controlling	Es el proceso en el cual se planifica y supervisa las operaciones del negocio	SAP

Reportes regulatorios

#	Unidad de negocio	Reporte	Descripción	País	Frecuencia	Entidad
1	Finanzas	608	Declaración de ITBIS	RD	Mensual	DGII
2	Finanzas	SAT-08	Declaración de IVA	GT	Mensual	SAT

Impacto Operacional

El impacto operacional será medido en la escala de 0 al 4 donde 0 = Muy bajo y 4 = Muy Alto. El valor de impacto de cada operación indica cuan severo seria el impacto a la compañía.

Operación	Valor
Flujo de Caja	4
Ventaja Competitiva	2
Confianza del cliente	2
Reportes financieros	4
Imagen del negocio	2
Moral del Empleado	4
Servicio al Cliente	2
Comisiones	4
Proveedores	4
Entidades Regulatorias	3
Otros	0

Numero del personal de recuperación requerido

El número del personal de recuperación por día, representa el número del personal interno requerido para esta unidad de negocios.

Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7	Día 14	Día 21	Día 28
4	4	4	4	4	4	4	4	4	4

MTO, RPO y RTO para Ventas

#	Procesos Críticos	Tiempo Máximo de Tolerancia (MTO)	Objetico de Punto de Recuperación (RPO)	Objetico de Tiempo de Recuperación (RTO)
1	Presupuesto	7 Días	5 Días	3 Días
2	Cuentas Por Cobrar	3 Días	2 Días	0.8 Días
3	Tesorería	6 Días	4 Días	2 Días
4	Controlling	4 Días	3 Días	2 Días

6. Recursos Humanos

Procesos

Para el propósito de este informe, solo fueron tomado en cuenta La gestión de Personal y Nomina donde se consideran parte de la función de Recursos Humanos.

#	Proceso de Negocio	Descripción	Herramientas
1	Gestión del Personal	En este proceso se Gestiona el personal de la empresa.	Eikon, Papel
2	Nomina	Es el proceso en el cual se realiza el pago de la nomina a los empleados	Eikon

Reportes regulatorios

#	Unidad de negocio	Reporte	Descripción	País	Frecuencia	Entidad
1	RRHH	IR-13	Declaración Agente de retención	RD	Anual	DGII
2	RRHH	IR-3	Declaración Liquidación de retención	RD	Mensual	SAT
3	RRHH	SAT-1063	Declaración Agente de retención	GT	Mensual	DGII

Impacto Operacional

El impacto operacional será medido en la escala de 0 al 4 donde 0 = Muy bajo y 4 = Muy Alto. El valor de impacto de cada operación indica cuan severo seria el impacto a la compañía.

Operación	Valor
Flujo de Caja	0
Ventaja Competitiva	3
Confianza del cliente	2
Reportes financieros	0
Imagen del negocio	4
Moral del Empleado	4
Servicio al Cliente	3
Comisiones	0
Proveedores	0
Entidades Regulatorias	3
Otros	0

Numero del personal de recuperación requerido

El número del personal de recuperación por día, representa el número del personal interno requerido para esta unidad de negocios.

Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7	Día 14	Día 21	Día 28
2	2	2	2	2	3	3	3	3	3

MTO, RPO y RTO para Ventas

#	Procesos Críticos	Tiempo Máximo de Tolerancia (MTO)	Objetico de Punto de Recuperación (RPO)	Objetico de Tiempo de Recuperación (RTO)
1	Gestión del Personal	12 Días	8 Días	5 Días
2	Nomina	9 Días	6 Días	4 Días

7. Tecnología de Información

Procesos

Para el propósito de este informe, solo fueron tomadas en cuenta La gestión de mensajería e internet donde se consideran parte de la función de Tecnología de Información.

#	Proceso de Negocio	Descripción	Herramientas
1	Mensajería	En este proceso en el cual permite un flujo de información entre los empleados.	Exchange
2	Gestión de uso del Internet	Es el proceso donde se crean y gestionan políticas y cuotas para el uso del internet	Isa server

Reportes regulatorios

#	Unidad de negocio	Reporte	Descripción	País	Frecuencia	Entidad
1	TI	N/A	N/A	RD	N/A	N/A
2	TI	N/A	N/A	GT	N/A	N/A

Impacto Operacional

El impacto operacional será medido en la escala de 0 al 4 donde 0 = Muy bajo y 4 = Muy Alto. El valor de impacto de cada operación indica cuan severo seria el impacto a la compañía.

Operación	Valor
Flujo de Caja	0
Ventaja Competitiva	3
Confianza del cliente	0
Reportes financieros	0
Imagen del negocio	4
Moral del Empleado	4
Servicio al Cliente	3
Comisiones	0
Proveedores	3
Entidades Regulatorias	0
Otros	0

Numero del personal de recuperación requerido

El número del personal de recuperación por día, representa el número del personal interno requerido para esta unidad de negocios.

Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7	Día 14	Día 21	Día 28
1	1	1	1	1	1	1	1	1	1

MTO, RPO y RTO para Ventas

#	Procesos Críticos	Tiempo Máximo de Tolerancia (MTO)	Objetico de Punto de Recuperación (RPO)	Objetico de Tiempo de Recuperación (RTO)
1	Mensajería	4 Días	2 Días	1 Días
2	Gestión de uso del Internet	6 Días	4 Días	2 Días

Reporte Ejecutivo del análisis de impacto de negocios

El Análisis de impacto de negocios (BIA) se ha diseñado para proporcionar una visión sobre los efectos generales para cada unidad de negocios de la empresa. Dado que el costo de recuperación, redundancia y tolerancia a fallos en la infraestructura puede ser

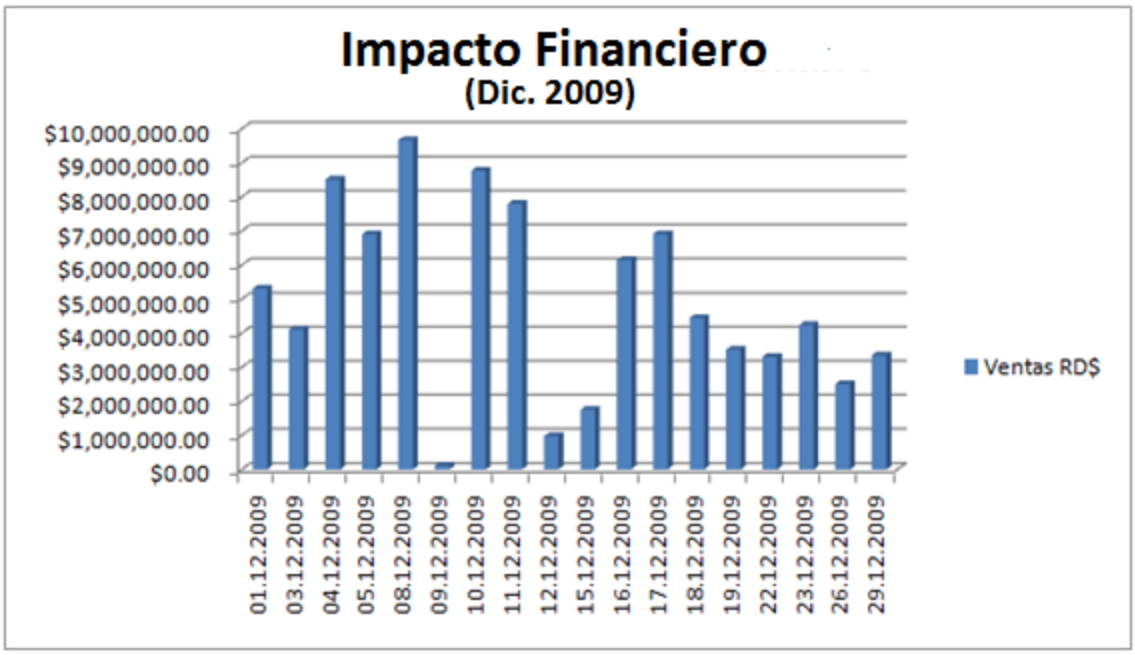
muy alta, por lo tanto es muy importante que la directiva de la empresa tenga una clara visión y el compromiso para llevar a cabo el trabajo.

El propósito de la siguiente sección es proporcionar un informe acumulativo de impacto en todas las unidades de negocios ya antes planteadas. Esta información sobre el impacto acumulativo puede ser aplicada para la justificación y la priorización de infraestructuras relacionadas con los recursos que serían necesarios.

2.3.2 Evaluación de impacto en la organización

Impacto Financiero Acumulativo

El siguiente grafico muestra el impacto financiero acumulativo que podría ocurrir para todas las unidades de negocios. A continuación se presentara un muestreo de un mes pico para así analizar las posibles pérdidas de la empresa.

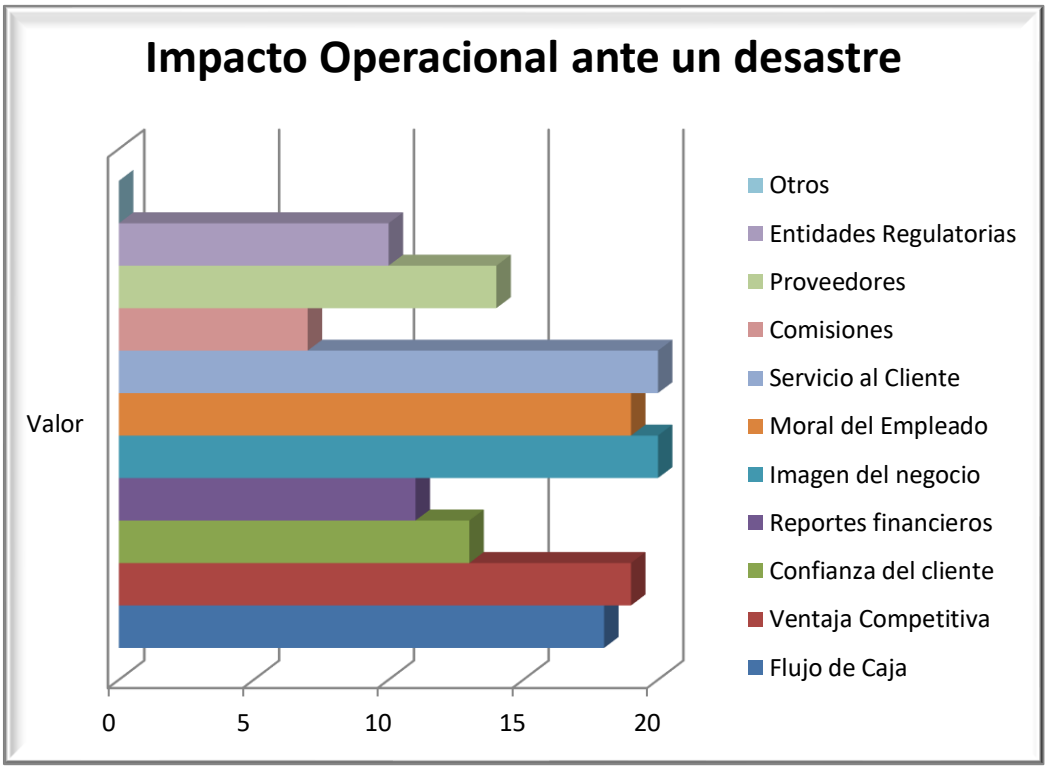


Hallazgos

El reporte financiero acumulativo tiene como rango entre $109,952.00 a $9,670,743.29 donde el pico más alto fue el 8 de diciembre.

Reporte acumulativo del impacto operativo

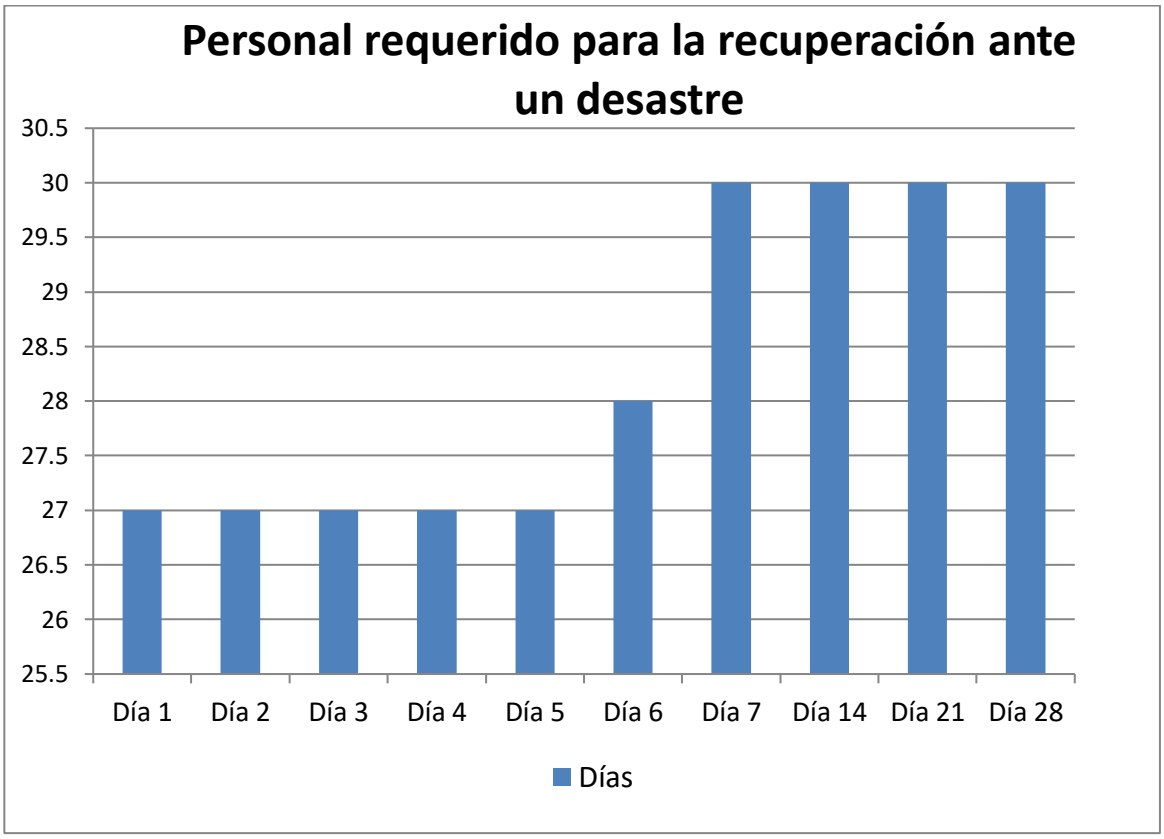
El impacto operacional es intangible y no se puede medir con precisión, pero sin embargo, utilizamos operaciones en común para todas las unidades de negocios donde tendríamos una visión de las operaciones que afectaría el negocio al momento de un desastre.



Hallazgos

Como se muestra en la grafica, el servicio al cliente y la imagen del negocio tienen mayor prioridad y son las que podrían afectar a todas las unidades del negocio.

Reporte acumulativo del personal requerido para la recuperación.



Hallazgos

De acuerdo con las entrevistas con los responsables de cada unidad de negocios, se necesitaría un aproximado de 30 personas en total para trabajar en la recuperación ante un desastre.

Actualmente la empresa tiene un total de 550 empleados.

Además, basado en las informaciones obtenidas en las entrevistas, los empleados actuales están en la disposición y capaces de trabajar fuera del horario de oficina para la reanudación de todas las operaciones de la empresa ante una catástrofe ocurrida. .

Reportes regulatorios

A continuación se muestra una lista de todos los formularios que demanda el estado de cada unidad de negocios.

#	Unidad de negocio	Reporte	Descripción	País	Frecuencia	Entidad
1	Ventas	6-07	Ventas de Bienes y/o Servicios	República Dominicana	Anual	DGII
2	Ventas	LVGT	Libro de ventas	Guatemala	Mensual	SAT
3	Logística	DUA	Declaración de Aduana	República Dominicana	diario	DGA
4	Logística	DUA	Declaración de Aduana	Guatemala	diario	SAT
5	Compras	707	Reporte compras de bienes y servicios	República Dominicana	Mensual	DGII
6	Compras	LCGT	Libro de compras	Guatemala	Mensual	SAT
7	Finanzas		Declaración de ITBIS	República Dominicana	Mensual	DGII
8	Finanzas		Declaración de IVA	Guatemala	Mensual	SAT
9	RRHH	IR-13	Declaración Agente de retención	República Dominicana	Anual	DGII
10	RRHH	IR-3	Declaración Liquidación de retención	República Dominicana	Mensual	SAT
11	RRHH	SAT-1063	Declaración Agente de retención	Guatemala	Mensual	DGII

2.3.3 Orden de recuperación recomendaciones

Según el análisis de impacto del negocio (BIA) realizado recomendamos que se realice el plan de recuperación de desastre (DRP) tomando este listado de procesos por orden de prioridad.

#	Proceso de Negocio	Unidad de negocio	Herramientas TI
1	Ventas Locales	Venta	SAP
2	Ventas Exportación	Venta	SAP
5	Despacho	Logistica	SAP, Exchange
6	Distribucción	Logistica	Excel, Software inhouse
11	Gestion de Ordenes de Procesos	Producción	SAP
13	Gestion de Calidad	Producción	Papel
15	Negociación y compra locales de bienes y servicios	Compras	SAP, Exchange
17	Negociación y compras internacionales de bienes y servicios	Compras	SAP, Exchange
19	Cuentas Por Cobrar	Finanzas	SAP
20	Tesoreria	Finanzas	SAP, Quicken
21	Controlling	Finanzas	SAP
24	Nomina	Recursos Humanos	Eikon
25	Mensajeria	Tecnologia de Información	Exchange
26	Gestion de uso del Internet	Tecnologia de Información	Isa server

2.3.4 Resumen Ejecutivo del BIA.

Para visualizar de manera más resumida el análisis de impacto del negocio, a continuación se muestra la siguiente tabla:

Químicos Dominicanos S.A.
(Quimidomsa)
Matriz de Análisis del Impacto sobre el negocio (BIA)

No.	Proceso / Aplicación	Descripción	Herramientas TI	Objetivo de tiempo de recuperación (RTO)	Impacto Financiero	Impacto en Clientes	Impacto legal / Regulatorio	Impacto a la Imagen corporativa
1	Ventas Locales	Es el proceso en el cual se realiza acuerdos de ventas con clientes locales.	SAP	0.7 Días	RD$5,500,000.00	A	A	A
2	Ventas Exportación	Es el proceso en el cual se realiza acuerdos de ventas con clientes extranjeros, donde se consideran otros recursos externos(aduanas, transporte, etc).	SAP	0.7 Días	RD$3,800,000.00	A	A	A
3	Ventas de Servicios	Es el proceso en el cual se realiza ventas de servicios tales como energia electrica y vapor que se generan en las instalaciones de Quimidomsa.	SAP	1 Días	RD$900,000.00	M	A	M
4	Despacho	Es el proceso en el cual se realiza y se gestiona las salidas de mercancias.	SAP, Exchange	0.7 Días	RD$215,000.00	A	B	M
5	Distribución	Es el proceso en el cual se coordina todo el transporte local y de exportación de las mercancias.	Excel, Software inhouse	1 Días	RD$450,000.00	A	B	M
6	Negociación y compra locales de bienes y servicios	Negociación con los vendedores y colocar ordenes de bienes y servicios de proveedores locales	SAP, Exchange	2 Días	RD$ 250,000.00	B	B	M
7	Negociación y compras internacionales de bienes y servicios	Negociación con los vendedores y colocar ordenes de bienes y servicios de proveedores Internacionales	SAP, Exchange	1 Días	RD$150,000.00	B	B	M
8	Gestión de Ordenes de Procesos	Es el proceso mendiante el cual se crean las ordenes de proceso, listado de herramientas y listado de recursos a utilizar para Producción.	SAP	2 Días	N/A	M	M	M
9	Gestión de Calidad	Es el proceso en el cual se garantiza la calidad de los productos realizados.	Papel	2 Días	N/A	B	B	B
10	Cuentas Por Cobrar	Es el proceso en el cual se gestiona los cobros de facturas a crédito con el proposito que se cumplan los pagos dentro del plazo establecido en el acuerdo de venta.	SAP	1 Días	RD$5,500,000.00	M	B	M
11	Tesorería	Es el proceso de planeación y el manejo de los fondos de la empresa en el corto, mediano y largo plazo.	SAP, Quicken	2 Días	N/A	M	M	M
12	Nomina	Es el proceso en el cual se realiza el pago de la nomina a los empleados	Eikon	4 Días	N/A	B	B	M
13	Mensajería	En este proceso en el cual permite un flujo de informacion entrre los empleados.	Exchange	1 Días	N/A	A	B	A
14	Gestión de uso del Internet	Es el proceso donde se crean y gestionan politicas y cuotas para el uso del internet	Isa server	2 Días	N/A	A	B	M

Escala: A (Alto) - M (Medio) - B (Bajo)

Capitulo 3: Diseño de estrategias de recuperación para el área de TI

3.1 Diseño de estrategias.

Determinar una buena estrategia para el Plan de Recuperación de Desastre (DRP) es un elemento clave y fundamental para garantizar una continuidad de negocios. Para lograrlo es necesario basarse en las fases de evaluación de Riesgos y el análisis de impactos de negocios (BIA) donde de acuerdo a los resultados de los controles existentes y sugeridos, además de los procesos críticos del negocio y sus tiempos requeridos para recuperación, nos mostrara el modelo ideal de estrategia que necesitaremos.

Las estrategias de recuperación están basadas obviamente en los resultados obtenidos luego de la realización del análisis de impactos de negocios (BIA), en donde se consideran los procesos críticos del negocio, el costo de de dicha estrategia la seguridad obtenida y los valores de los tiempos máximos permitidos de no disponibilidad (MTD).

En la determinación de la estrategia se busca:

- Reducir consecuencias negativas.
- Reducir la probabilidad de que ocurra.
- Disminuir la amenaza a cualquier desastre

Opciones de estrategias

Para determinar qué estrategia de Recuperación es la más factible para la empresa se debe conocer las opciones existentes para su selección. En esta fase se debe asegurar que las opciones de Recuperación estén alineados con las necesidades y requerimientos de la empresa, tanto el costo como también los beneficios de dicha estrategia.

Existen diferentes opciones de estrategias para la recuperación, para este proyecto señalaremos las más usuales, que son:

1. **Hot Site**, Es un duplicado del sitio original de una organización, Listo para operar en pocas horas, tiene equipos, red y sistemas necesarios.

   Casi siempre se utiliza sincronización en tiempo real entre los dos data centers para lograr una copia del ambiente original.

   Luego de una interrupción del sitio original, el Hot Site existe para que la organización pueda trasladar con pérdidas mínimas de operaciones normales.

2. **Warm Site**, Es un lugar (centro de datos/ área de trabajo) equipado parcialmente con "hardware", interfaces de comunicaciones, electricidad, y acondicionamiento ambiental con capacidad de proveer soporte operacional de respaldo.

   Este puede operar en menos de un día. Esta parcialmente configurado, con conexiones de red y equipos seleccionados. Con capacidad de CPU menor a la de producción.

3. **Cold Site**, Consiste en Un lugar (área para la central de datos/lugar de trabajo) equipado con condiciones ambientales apropiadas, conexiones eléctricas, acceso a comunicaciones, espacio configurable, y facilidad de instalar y operar equipo por el personal clave requerido para resumir las operaciones del negocio.

   Este site no incluye copia de la data, ni tampoco incluye hardware preparado para la pronta implementación en caso de desastre.

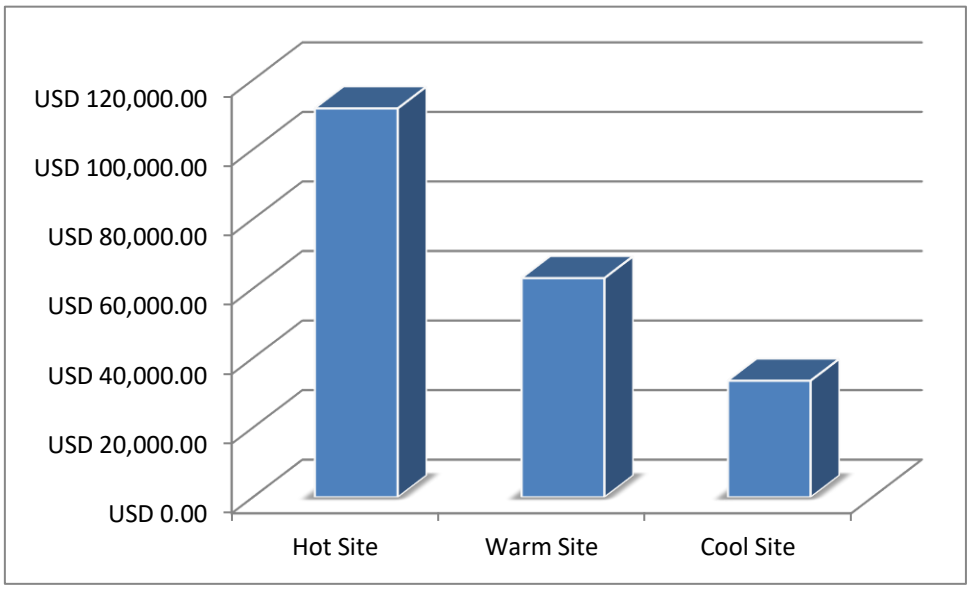
3.2 Análisis de alternativas de estrategias de DRP.

Es imposible juzgar el coste adecuado de las medidas mediante un análisis de coste-beneficio convencional debido a que es necesario asumir premisas cuestionables acerca de la probabilidad de los incidentes para demostrar que existen beneficios.

Para la selección de la estrategia de recuperación se realizo la siguiente tabla donde muestra los costos de cada opciones con el propósito de evaluar cual sería la más factible, considerando su retorno de inversión a la empresa.

Tabla. Costos[1]

Opciones	Costos HW &SW	Costo Implementación	Total
Hot Site	USD 55,790.00	USD 56,000.00	USD 111,790.00
Warm Site	USD 38,500.00	USD 24,500.00	USD 63,000.00
Cool Site	USD 15,500.00	USD 18,000.00	USD 33,500.00



[1] Ver en Apéndice IV la lista completa de costos.

Según los resultados de estos costos, el más costoso es el Hot Site ya que para mantener esta alternativa requiere un esfuerzo continuo y herramientas de transferencia a tiempo real.

Para un mejor entendimiento y comparación acerca de las diferentes alternativas existentes.

Categoría	Hot Site	Warm Site	Cold Site
Disponibilidad	minutos a horas	Horas a Días	Días a semanas
Sistema de aplicación	Cargar y Listo	Presente pero no está listo	NO presente, se deberá comprar e instalarlo
Datos de Aplicación	Hasta la fecha	No al día; se necesita hacer un refresh	No presente, debe estar cargada.
Costo	Muy Alto	Moderado	Muy Bajo.

3.3 Definición de las estrategias de DRP.

De acuerdo al análisis realizado sobre las diferentes estrategias, donde se consideraron los costos y el alcance de dichas alternativas de estrategias, llegamos a una conclusión de acuerdo a las siguientes premisas:

- La directiva de Quimidomsa ha asignado un presupuesto de USD$ 61,000.00 para la realización de la estrategia utilizada para este proyecto.
- La directiva de Quimidomsa está de acuerdo en implementar un Plan Recuperación de Desastre (DRP) para los procesos críticos de la empresa. Según el inventario de recursos de TI, nos damos cuenta que el 80% de los procesos críticos están instalados en solo sistema, llamado SAP.
- SAP, trabaja bajo las plataformas de varios recursos, en este caso de Servidores y Almacenamiento SAN. De acuerdo a los controles sugeridos, se recomendó la utilización de dos NAS, el primero en el site principal y el segundo externo. Esta recomendación se considero como válido para la elaboración de la estrategia.

- Los sistemas restantes, solo se consideraran el sistema de Nomina y de mensajería de acuerdo al análisis de impacto de negocio (BIA), donde refleja que estos dos son herramientas utilizadas para los procesos críticos del negocio.

De acuerdo a estas premisas y tomando en consideración el presupuesto versus los costos de las alternativas descriptas anteriormente, recomendamos utilizar la opción de un **Hot Site** ubicado en la sede de Guatemala, donde actualmente cuenta con un data center apto para dicha utilización.

El Hot Site tendría una imagen espejo virtual de la sede principal, con todos los sistemas críticos configurados. Se recomienda esta estrategia por los siguientes factores:

- **Tiempo de Recuperación:** Al estar la sede secundaria fuera del país, a una distancia de 6 horas y sumándole el tiempo necesario para la recuperación de todos los procesos, es necesario asegurar el objetivo de tiempo de recuperación (RTO) contando una copia fiel en tiempo real de la sede principal.

- **Robustez:** Este Puede garantizar al momento de que algún proceso critico sufra un fallo, este a pesar de ello puede seguir operando.

- **Integridad:** Garantiza la fiabilidad de los datos, esto se deberá por la sincronización de los datos entre las dos sedes en tiempo real.

Activos requeridos

Para el **Hot Site** se requiere los siguientes activos:

- **Hardware**

Hardware	Descripción
Servidor SAP	Servidor de aplicaciones SAP
NAS	Almacenamiento del Sistema SAP
Servidor de Virtualización	Servidor donde estaran alojados varios servidores virtuales
Equipos de Comunicación	Swith, Router, Cabledos
RACK	Base para protección de los servidores

- **Software**

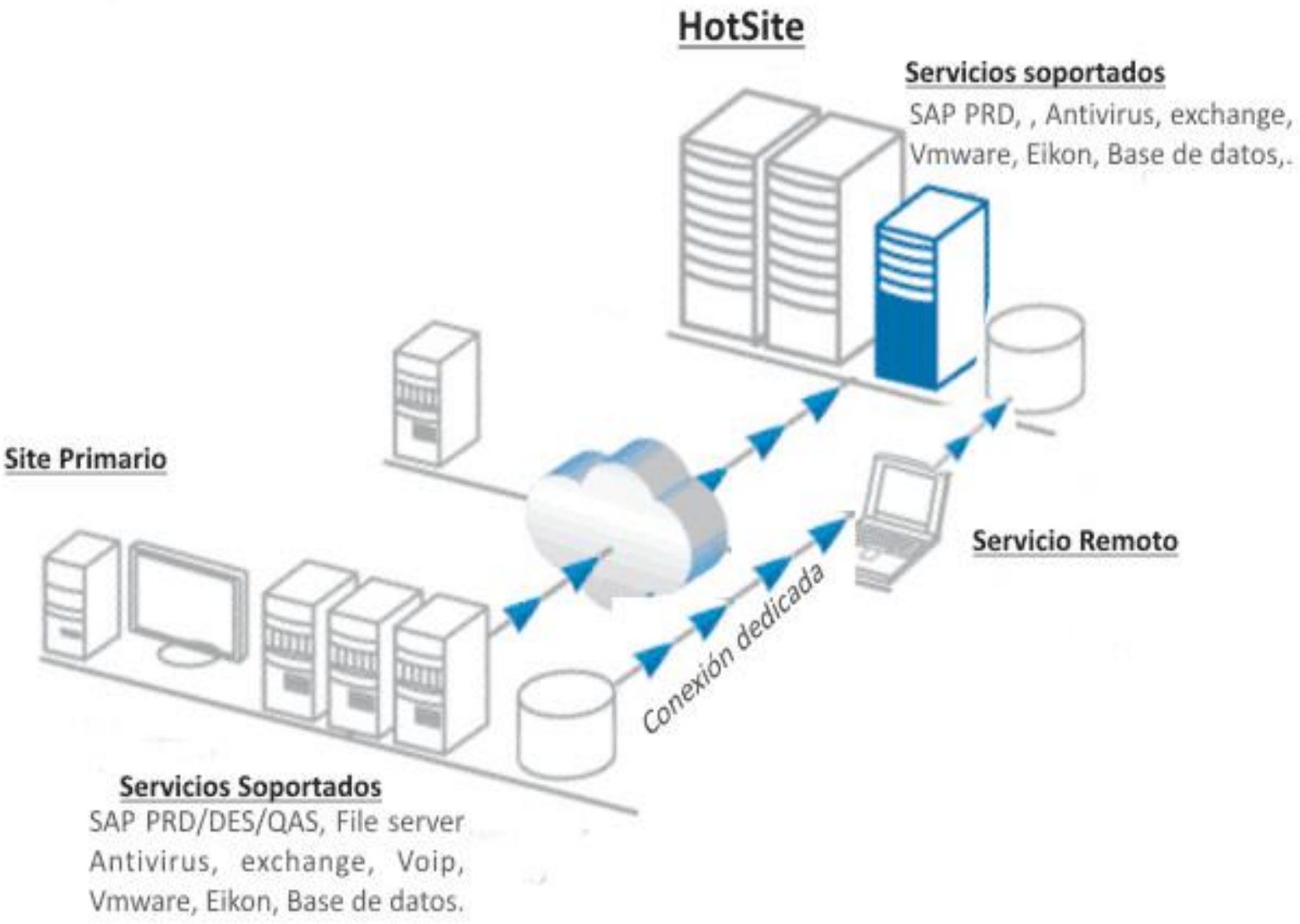
Software	Descripción
SAP Mandante Productivo	SAP ERP 5
AntiVirus & AntiSpam	Symantec Antivirus
Eikon	Gestion de RRHH & Nomina
Exhange	Gestion de Correo Electronico

- **OS**

istema Operativo	Licencias
Windows Server 2003	5

- **Base de Datos**

Base de datos	Cantidad
Microsoft SQL Server Enterprise Edition	2
Microsoft SQL Server Standard Edition	4


HotSite
Servicios soportados
SAP PRD, , Antivirus, exchange,
Vmware, Eikon, Base de datos,.
Site Primario
Servicio Remoto
Conexión dedicada
Servicios Soportados
SAP PRD/DES/QAS, File server
Antivirus, exchange, Voip,
Vmware, Eikon, Base de datos.

Políticas de Backup y recuperación.

Para asegurar una buena estrategia de recuperación se requiere que se realicen las siguientes políticas para el Respaldo y recuperación de datos.

El programa de backups es el siguiente:

Servidor	**Frecuencia**	**Hora**	**Tipo de backup**
QMDDEV (SAP R/3 – Desarrollo)	Lunes a viernes	4:00 PM	Full máster backup Full MSDB backup
QMDPRD (SAP R/3 - Productivo)	Lunes a viernes	10:00 PM	Full máster backup Full MSDB backup
QMDPRD (SAP R/3 - Productivo)	Lunes a viernes	Cada 1 hora	Transaction Log
QMDMAIL (Dominio y Correos)	Lunes a viernes	12:00 PM	Backup de configuración Backup de buzón
QMDRPS (Archivos e impresoras)	Lunes a viernes	10:00 PM	Backup de archivos
QMDSDC(Backup del dominio, antivirus y Data Protector)	Lunes a viernes	10:00 PM	Backup de archivos
QMDRRHH(Sistema Nomina)	Lunes a viernes	10:00 PM	Backup Base de datos
QMDSCAM (Backup del Grabaciones de Cámaras de Seguridad)	Lunes a viernes	10:00 PM	Backup de archivos
QMGTFILE (Backup File server)	Lunes a viernes	10:00 PM	Backup de archivos
QMGTRRHH (Backup Sist. Nomina)	Lunes a viernes	10:00 PM	Backup Base de datos

Cada cinta de backup posee una identificación única según la siguiente tabla

Servidor	**Juego de cintas**	**Cinta de emergencia**
QMDDEV (SAP R/3 - Desarrollo)	BKGMD1 BKGMD4 BKGMD2 BKGMD5 BKGMD3 BKGMD6	BKGMD10
QMDPRD (SAP R/3 - Productivo)	BKGMP1 BKGMP5 BKGMP2 BKGMP6 BKGMP3 TRLOG1 BKGMP4 TRLOG2	BKGMP10
QMDMAIL (Dominio y Correos)	BKBZE1 BKCFGE1 BKBZE2 BKCFGE2 BKBZE3 BKCFGE3 BKBZE4 BKCFGE4 BKBZE5 BKCFGE5 BKBZE6 BKCFGE6	BKBZE10 BKCFGE10
QMDFILE (Archivos e impresoras)	BKGMDF1 BKGMDF2 BKGMDF3 BKGMDF4 BKGMDF5 BKGMDF6	BKGMDF10
QMDSDC(Backup del dominio)		
QMDRPS(File Server)		

Processo de Realización de backups

- Los backups de los diferentes servidores se realizan de manera automática a través de la aplicación Data Protector. En esta aplicación se define el programa de backups y sólo es necesario colocar las cintas en la unidad de backup correspondiente. Las cintas se colocan cada día en la unidad de backup siguiendo la numeración secuencial.

- Diariamente, el Administrador de Sistemas & Redes verifica que los backups programados se realicen correctamente. Para ello, revisa el registro de la aplicación Data Protector. Si el backup no se realizó correctamente, el Administrador de Sistemas & Redes realiza el backup manualmente. Este proceso continua hasta que el backup se realice correctamente.

- Las cintas de backup se almacenan fuera de la empresa. Al final de cada día, el Administrador de Sistemas & Redes entrega al Gerente de Proyectos & Tecnología el juego de backup correspondiente que contiene 5 cintas. Al momento de entregar el juego de cintas, el Administrador de Sistemas & Redes completa el formulario Control de cintas de backup FO-011, donde el Gerente de Proyectos & Tecnología firma como acuse de recibo. Las cintas de backup son entregadas al Vicepresidente o Presidente de la organización cuando el Gerente de Proyectos & Tecnología esté ausente.

- Cada martes, el Gerente de Proyectos & Tecnología entrega al Administrador de Sistemas & Redes todo los juegos de cintas de backup que estaban almacenados fuera de sito, excepto el juego de cintas de backup del lunes.

Pruebas de Recuperación

Se efectuarán pruebas de recuperación de las copias de respaldo por parte del administrador de servidores al menos una vez cada 90 días y serán supervisadas por el administrador de aplicaciones. Además se tomaran muestras representativas de los meses anteriores para su prueba.

Estas pruebas servirán para constatar que se puedan obtener correctamente los datos grabados en la cinta al momento de ser necesarios, de forma de garantizar su propósito.

Las pruebas se deberán formalizar en un acta escrita y firmada por el responsable del sector técnico y el encargado de realizar la recuperación. Eventualmente el área responsable del la seguridad tecnológica presenciará las pruebas y firmará el acta.

Capitulo 4: Desarrollo e Implementación del Plan de Recuperación de desastres para TI

4.1 Objetivo del Plan

En el Plan de Recuperación de Desastres (DRP) para el área de TI, se define cómo deberán recuperarse los servicios críticos de TI que se utilizan en una organización ante un desastre, incluyendo las diferentes alternativas procedimentales, recursos humanos y soluciones tecnológicas posibles.

Aspectos a considerar

- El desarrollo del plan de recuperación de desastres (DRP) se realizó basado en los resultados del análisis de riesgos y el de impacto del negocio, y se enfoca en las estrategias de recuperación seleccionadas por la gerencia.
- El plan abarca todas las posibles incidencias que se contemplaron en el análisis de riesgo, no solamente las que poseen un riesgo más alto, con esto tratamos de abarcar la mayor cantidad de desastres posibles.

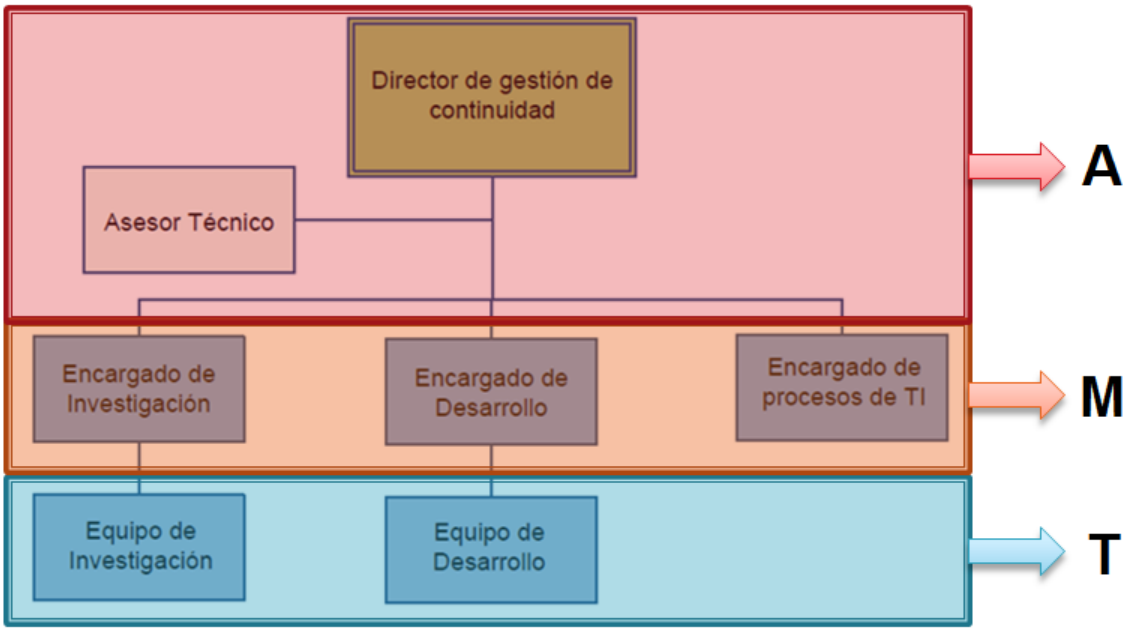
El objetivo por el cual se debe preparar un plan de recuperación para el área de TI es justo para que esta parte crítica de la organización pueda contar con un modelo de recuperación y con la infraestructura necesaria para restaurar las operaciones de la empresa que dependa del área de TI, en caso de presentarse una contingencia o un desastre en el Centro de Cómputo que imposibilite cumplir con los niveles de servicio comprometidos.

4.2 Responsables del plan recuperación de desastre (DRP)

En el capítulo 1.7 presentamos el organigrama de cómo debería estar compuesto el equipo encargado de manejar y trabajar con la implementación del plan de continuidad para la empresa Quimidomsa, sin embargo la responsabilidad es de toda la organización, ya que es un esfuerzo común que se debe realizar para poder lograr una verdadera cultura de continuidad.

Dentro de cada departamento de la empresa es necesario contar con personas a los cuales se puede acudir en caso de incidentes, estas personas estarán dotadas de los procedimientos o acciones a tomar para cada tipo de incidente o en su defecto a quien recurrir para que pueda tomar la acción, ya que dependiendo del incidente se estarán asigna do los niveles de autorización para poder llevar a cabo una acción.

Los niveles de aprobación del plan vendrán dados acorde al siguiente esquema.



Las letras y colores indican los siguientes niveles de aprobación basados en las estrategias.

A – Alto Nivel **M – Nivel Medio** **T – Nivel Técnico**

A – Alto Nivel

El tipo de autorización requerida para los incidentes que impacten directamente las operaciones del negocio, A este tipo de autorización son generalmente asociados altos costos de la estrategia a implementar o el impacto que las decisiones puedan provocar. (Solo puede ser otorgada por el Director de Continuidad o los Directivos de la empresa).

M – Nivel Medio

Este tipo de aprobación la pueden otorgar los encargados de los equipos de continuidad de la empresa, La aprobación de un nivel medio no necesariamente produce un impacto en el costo de la estrategia utilizada, sin embargo puede resultar vital el impacto organizacional de este tipo de aprobación.

T – Nivel Técnico

Es la aprobación realizada por los supervisores y líderes de equipo, están relacionados a incidentes menores y de poca relevancia dentro de la empresa.

Ahora veamos los niveles de acuerdo a un esquema similar al análisis de riesgo:

		Impacto				
		Mínimo	Menor	Moderado	Mayor	Catastrófico
Costo	Imperceptible	T	T	T	M	M
	Mínimo	T	T	T	M	A
	Aceptable	T	T	M	A	A
	Elevado	T	M	M	A	A
	Muy elevado	M	M	A	A	A

Viendo el esquema anterior claramente podemos notar que el tipo de estrategia o acción a tomar deben ser autorizadas bajo cierto criterio ya que implican un costo y producen un impacto en la organización, cabe mencionar que el impacto al cual nos referimos es el mismo impacto que nos produce el incidente al cual nos enfrentamos. Ejemplo, si nos referimos a un huracán el impacto puede ser catastrófico, y los costos por mínimos que sean deben ser autorizados por la dirección de la empresa. Sin embargo si fuese un simple derrame de materiales en la planta de producción, el impacto sería mínimo y a menos que conlleve un costo muy elevado, la acción puede ser realizada por el personal de supervisión.

Roles y responsabilidades

Es una táctica importante la distribución de las responsabilidades y asignaciones, de este modo evitamos cometer el error de que un proceso o una acción dependa únicamente de una persona.

Con esta acción ayudamos a la consecución de los objetivos de la empresa salvaguardando o preservando un área en particular, si todos cooperan la carga se aliviana.

Equipos propuestos:

Los equipos propuestos se dividen en cuatro grupos:

- Entorno y provisiones
- Gerenciales
- Recursos Humanos
- Sistemas y soporte TI

Objetivos generales de los equipos:

- Minimizar la interrupción de las operaciones normales de Quimidomsa.
- Limitar la extensión de la pausa o el daño.
- Minimizar el impacto económico de la interrupción.
- Proveer una suave y rápida restauración de los servicios.

Equipos de Entorno y provisiones

Son los encargados de velar el entorno de las instalaciones, la infraestructura, las condiciones para seguir operando, que las provisiones, suministros, materiales y otras herramientas de trabajo se encuentren en estado normal para continuar las operaciones.

Entre los equipos que componen este grupo están:

- Equipo de determinación de los daños.
- Equipo de Transporte.
- Equipo de suministros.

Equipos Gerenciales

Estos equipos son los encargados de ofrecer soporte a la gerencia, en los aspectos de políticas, reglas, normas, regulaciones o cualquier otro impase legal; del mismo modo en estos equipos se encargan de proteger y actualizar los reglamentos, políticas, formularios, contratos internos y otros documentos importantes para la organización. Finalmente tienen la voz cantante en el proceso de recuperación ya que son quienes indicaran o autorizaran las acciones en cada fase del proceso de recuperación y son los únicos encargados de externar algún tipo de información a los medios.

Dentro de este tipo figuran los equipos:

- Equipo de soportes, datos y registros.
- Equipo de trámites Legales.
- Equipo de Recuperación
- Equipo de coordinación de medios y prensa

Equipos de Recursos Humanos

Es el equipo encargado de velar por el bienestar de los recursos humanos en caso de algún incidente, tanto en asistencias médicas y salvamento, como en seguridad. Del mismo modo son estos equipos los encargados de coordinar los procesos reubicación en caso de ser necesarios.

Hacemos mención de estos equipos:

- Equipo de operaciones de emergencia y salvamento.
- Equipo de seguridad.
- Equipo de coordinación y reubicación.

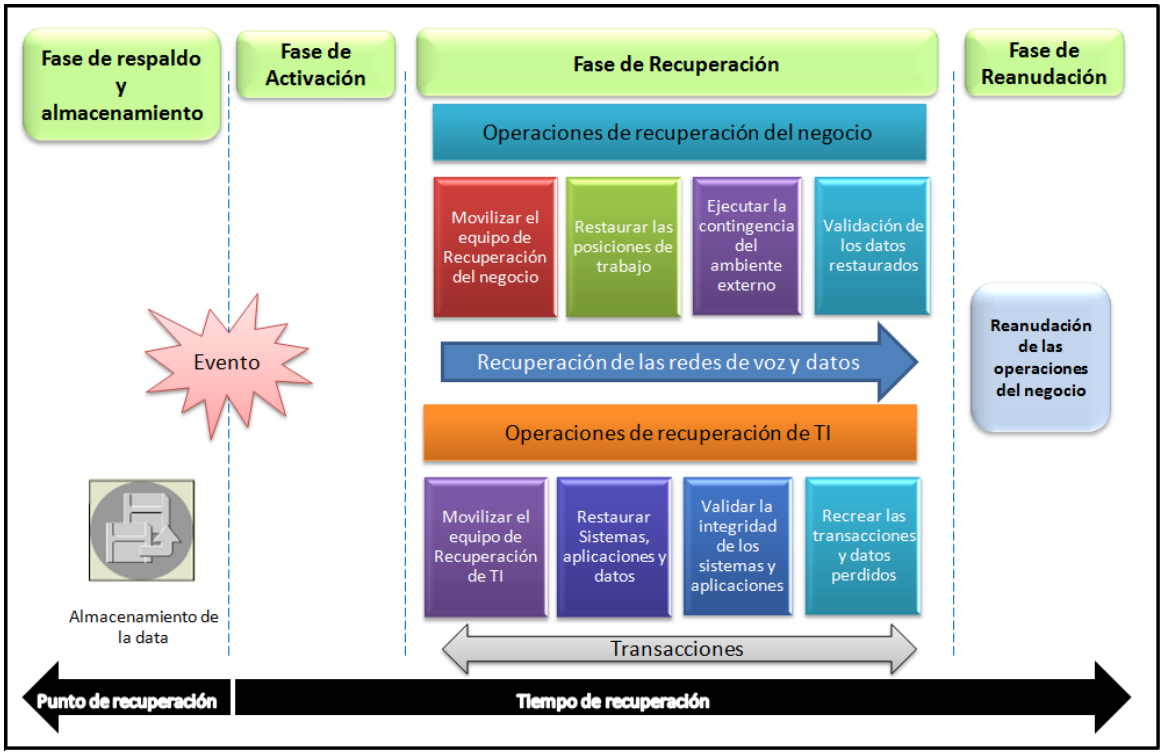
Equipos de Sistemas y soporte TI

Son estos equipos los más importantes en todo el proceso de recuperación ya que son los que mantienen el flujo de las operaciones en su curso normal. Estos equipos son:

- Equipo de almacenamiento y respaldo.
- Equipo de software.
- Equipo de recuperación de red.
- Equipo de Comunicaciones.
- Equipo de Hardware.

4.3 Definición de la estructura y formato del Plan

Antes de ampliar sobre las funciones y roles de los equipos que impactan el área de TI, veremos cuáles son las fases que se presentan desde el momento de la ocurrencia de un incidente.



Lo que esta gráfica nos explica son los distintas fases que componen el proceso de recuperación:

- **Respaldo y Almacenamiento:** Esta es la fase previo a la ocurrencia de algún incidente, en esta parte se definen el modo en que se estará respaldando la información de la compañía y como se estará realizando el almacenamiento de dichos respaldos.
- **Activación:** En esta parte se define el punto de partida de mi plan de recuperación, Antes de activar el plan se deberá definir en qué momento aplicarlo, es decir qué se considerará un escenario de desastre o contingencia que afecte el área de TI.

- **Recuperación:** Esta es la fase más amplia ya que abarca la preparación del ambiente, la puesta en marcha de las aplicaciones así como la recuperación del flujo de datos y procesos dentro de la compañía.
- **Reanudación:** En esta fase se definen las actividades para el retorno de las operaciones normales de la empresa, así como el cierre reinicio de los centros y servicios alternos que fueron definidos en caso necesario.

En resumen, las fases conllevan los siguientes pasos:

Reducción	**Respuesta**	**Recuperación**	**Reanudación y Regreso**
Mitigar, planear y prevenir **ANTES** del desastre	Implementar Procedimiento de respuesta **DURANTE** el desastre	De las operaciones y procesos críticos **DESPUES** del desastre	A las operaciones normales en la localidad final

Tabla RACI del proceso general de recuperación del área de TI.

Proceso:	**DRP en el área de TI**

Paso	Acción	Equipo de gestión de continuidad	Equipo gerencial	Equipo de sistemas y soporte TI	Equipo de Recursos humanos	Equipo de Entorno y provisiones
1	Almacenar y respaldar la data	**A**		**R**		
2	Identificar un incidente	**R,A**	**I**	**R**		
3	Reportar y evaluar el incidente	**R**	**A**	**C**	**C**	**C**
4	Activar el plan de recuperación	**A**	**R**			
5	Movilizar los equipos	**R**	**A,I**	**C**	**C**	**I**
6	Preparar el ambiente	**A**	**I**	**R**		
7	Preparar las aplicaciones e infraestructura	**A**	**I**	**R**		
8	Reiniciar el flujo de operaciones	**A**	**I**	**R**	**R**	
9	Evaluar los daños del incidente	**A**	**I**	**C**	**C**	**R**
10	Evaluar impactos del incidente	**A**	**R,A**	**C**		
11	Restauración de las operaciones	**A**	**I**	**R**	**R**	**C**
12	Documentación del incidente	**R,A**	**I,C**	**C**	**C**	**C**

R	**Realiza la acción**
A	**Responsable de que se complete la acción**
C	**Consultado para completar la acción**
I	**Informado cuando se complete la acción**

Esta tabla se denomina RACI por las iniciales en Ingles de los identificadores que Utiliza, siendo estos R – Responsible; A – Accountable; C – Consulted; I – Informed.

En español la traducción sería: R – Responsable; A – Aprobador; C – Consultado; I - Informado

En la tabla anterior se definen las personas encargadas de la acción establecida, también las personas responsables de que está acción se complete, las personas que son consultadas durante el proceso e incluso a que personal se debe de informar sobre la acción realizada.

4.4 Definición de los componentes y contenido del plan

El plan de recuperación de desastres contiene lo siguiente:

- Los análisis de riesgo e impacto (RA y BIA)
- Copia de los contratos, procedimientos, políticas y normas de la empresa
- Originales de cualquier formulario manual que sea utilizado en los procesos
- Diagramas de la configuración física y lógica de los equipos de TI (Tanto del site original como del alterno)
- Diagramas de las conexiones eléctricas y telefónicas (Tanto del site original como del alterno)
- Listado de activos del área de TI
- La última actualización del Control de cintas de backup FO-011
- Listas de los equipos con sus integrantes
- Listas de contactos (Clientes, suplidores, personal crítico, etc.)
- Lista de actividades durante un incidente
- Lista de actividades luego de un incidente

4.5 Determinación de la logística para la documentación

Luego de completado el proceso de recuperación, es necesario realizar la documentación del proceso que se concluyo para su estudio y verificación y que este pueda servir de precedente para futuras situaciones.

¿Qué se debe realizar antes de documentar?

- Entrevistas (estructuradas y no estructuradas), con todo el personal involucrado en el proceso de recuperación
- Realizar un nuevo Análisis del Impacto en el Negocio (BIA) y un nuevo análisis de riesgo (RA) con el objetivo de evaluar si existe mucha variación en relación a los anteriores.
- Nuevas listas de verificación, contactos y formularios (En caso de que sea necesario)
- Talleres con todo el personal involucrado en el proceso de recuperación de TI

¿Qué se debe documentar y evaluar?

- Se deben documentar los checklist o lista de actividades de cada equipo, para identificar si una de las labores realizadas por estos no estuvo acorde a lo planteado.
- La lista de componentes que se actualizó
- Cómo y quién tomó las decisiones en casa parte del proceso.
- Como se realizó la movilización de recursos
- Todos los documentos e informes recibidos y realizados durante el proceso de recuperación.
- Lista de los recursos utilizados y detalle de los recursos disponibles
- Listado de personal con sus respectivas informaciones
- Datos de las Instalaciones y suministros (En caso de que haya variación)
- Datos de la Tecnología, comunicaciones y datos (En caso de que haya variación)
- Nuevas políticas de seguridad (De ser requerido)
- Nuevas políticas de Transporte y logística (De ser requerido)
- Listados y facturas de las necesidades básicas, consumos y pagos de emergencia realizado por el personal involucrado en la recuperación.

- Listado de los recursos humanos y las funciones que se necesitaron para la recuperación de cada actividad.
- Información de clientes actuales (En caso de que haya variación)
- Detalles de los contactos (En caso de que haya variación)
- Documentos legales (contratos y pólizas de seguro en caso de que haya variación)
- Detalle de los Acuerdos de servicios

4.6 Elaboración documentada del plan de recuperación para el área de TI.

El plan de recuperación debe ser lo más explicito posible, con el objetivo de que cualquier persona que lo lea pueda fácilmente comprenderlo.

Toda la documentación que conlleva el plan de recuperación puede ser dividida en tres ramas:

- **Documentación de Actividades:** Se colocan las acciones y responsabilidades de cada uno de los equipos que conforman el equipo de recuperación.

- **Documentación de Procedimientos:** Se colocan los listados de actividades para cada situación de emergencia, y para cada momento, durante y después de un incidente. (Ver capitulo 4.8). En esta parte también deben estar los diagramas de conexiones eléctricas, telefónicas, y de configuraciones física y lógica de los equipos de la empresa, así como las copias de los contratos, procedimientos, políticas y normas.

- Reportes y formularios: Se colocan todo los formularios originales de cualquier transacción manual que sea utilizado en los distintos procesos, debe contener el Listado de activos del área de TI, y las diferentes listas.

Plantillas sugeridas para los diferentes listados

Listado de distribución, donde se especifican la cantidad de copias que se han realizado del plan, con el nombre de la persona que la posee, su departamento y ubicación y un teléfono de contacto.

# de la copia	Nombre	Ubicación / Departamento	Teléfono
1			
2			
3			
4			
5			

Listado de equipos del plan, uno para cada equipo donde se indican las personas responsables y corresponsables y luego el listado completo de integrantes.

Nombre del equipo:	
Responsable:	
Corresponsable:	

Nombre	Posición	Departamento	Teléfono

Listado de personal crítico, En este tipo de listado generalmente se colocan los datos de los altos directivos de la empresa, y en algunos casos asesores, abogados y consultores externos.

En caso de que el personal sea interno solo se han de colocar los nombres, teléfonos y dirección. Pero en caso de ser personal externo es requerido colocar todos los datos de la plantilla. El campo de acción se refiere al área en particular en la que puede ayudar o asesorar la persona.

Nombre	Teléfono	Email	Dirección	Campo de acción

Listado de personal de emergencia, En este listado se deben colocar todos los números de las instituciones de emergencia y proveedores de servicios básicos. En el campo de referencia se coloca el nombre del contacto interno entre la institución y la compañía.

Contacto	Número	Referencia
Policía	809-682-2152	Opc 0
Bomberos	809-682-2000	
Escuadrón Antibombas	809-530-5149	(Antimotines)
Paramédicos	809-535-1080	Movimed
Compañía de seguros	809-960-7200	Opc 1 (Seg. Banreservas)
Agua	809-562-3500	
Gas	809-227-0003	Tropigas
Electricidad	809-683-9393	EDE-ESTE
Teléfono	809-220-1111	Codetel

Listado de suplidores, proveedores y contratistas, se recomienda colocar dos opciones de cada tipo ya que dependiendo del incidente puede que una de estas se encuentra inmersa en la misma situación. El horario y el tipo de servicio son datos muy importantes dentro de este listado.

Empresa	Teléfono	Horario	Dirección	Tipo de servicio

4.7 Actividades del plan

Las actividades que debe realizar cada equipo varían entre cada uno, a continuación indicaremos los objetivos de los equipos encargados de la recuperación y un análisis detallado de las funciones especificas del equipo de TI.

Objetivos de los equipos de entorno y provisiones

- Identificar daños de infraestructura en las instalaciones
- Validar la factibilidad de condiciones para operar en el lugar afectado
- Mantener un control e inventario de los suministros, provisiones, materiales y herramientas de trabajo
- Velar y mantener disponibles los vehículos de la empresa
- Realizar el transporte de personal, equipos, suministros, materiales y provisiones en caso de ser necesario.
- Apoyar en el proceso a cualquier equipo que así lo requiera.

Objetivos de los Equipos gerenciales

- Velar por la documentación y almacenamiento de las políticas, reglas, normas y regulaciones vigentes en la compañía
- Asegurarse de que durante el proceso de recuperación no se incumpla ningún reglamento o regulación que provoque un impase legal
- Analizar las estadísticas del proceso de recuperación (Análisis de costos, pérdidas, etc.)
- Comunicar el estado de la empresa a los empleados, clientes y a los medios.

Objetivos de los equipos de recursos humanos

- Proveer seguridad a la empresa
- Velar por el bienestar de los recursos humanos en caso de algún incidente, ofreciendo asistencias médicas o labores de rescate y salvamento
- Ofrecer asistencia psicológica durante y después de un incidente
- Coordinar los procesos reubicación en caso de ser necesarios
- Orientar y dirigir a los contactos externos al momento de acceder a la empresa. (Policías, bomberos, suplidores, etc.)

Objetivos de los equipos de sistemas y soporte TI

Los objetivos de los equipos de sistemas y soporte de TI los estaremos analizando por separado con mayor detalle, a continuación mostraremos una tabla RACI que expresa la relación de responsabilidades entre los equipos.

Equipo	**Sistemas y soporte TI**
Fecha	******

Paso	Acción	Equipo de gestión de continuidad	Almac. y respaldo	Software	Recuperación de red	Comunic.	Hardware
1	Almacenar y respaldar la data		**R**				
2	Identificar un incidente	**R,A**	**R,I**	**R,I**	**R,I**	**R,I**	**R,I**
3	Reportar y evaluar el incidente	**R**	**I**	**I**	**I**	**I**	**I**
4	Activar el plan de recuperación	**R**					
5	Movilizar los equipos de TI	**R**	**I**	**I**	**I**	**I**	**I**
6	Realizar las procedimientos de recuperación	**A**	**R,I**	**R,I**	**R,I**	**R,I**	**R,I**
7	Reiniciar el flujo de operaciones	**A**	**R,I**	**R,I**	**R,I**	**R,I**	**R,I**
8	Restauración de las operaciones	**A**	**R,I**	**R,I**	**R,I**	**R,I**	**R,I**
9	Mantenimiento de las operaciones	**A**	**R**	**R**	**R**	**R**	**R**

R	**Realiza la acción**
A	**Responsable de que se complete la acción**
C	**Consultado para completar la acción**
I	**Informado cuando se complete la acción**

Las acciones indicadas en color azul son acciones cuya responsabilidad recae sobre el equipo que presente impacto, y luego de terminar la acción debe informar cuando la haya completado. Ejemplo: Si un incidente produce un impacto en la red, el equipo de recuperación de red será el responsable de identificar cual es el incidente, realizar el procedimiento de recuperación establecido para este equipo para reiniciar el flujo de las operaciones, finalmente deben indicar cuando ya todo debe volver a la normalidad.

Desglose de actividades por equipo

Equipo de almacenamiento y respaldo

ACCIÓN A REALIZAR ANTES DEL INCIDENTE	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Realizar los backups acorde a las políticas vigentes y con el software correspondiente	❑	
Entregar los juegos de cintas al personal correspondiente para fines de almacenamiento	❑	
Completar el formulario FO-011 de control de cintas de backup	❑	
Realizar un inventario semanal de las cintas en stock	❑	
Realizar las pruebas y mantenimientos acorde a los esquemas establecidos	❑	
ACCIÓN DE RECUPERACIÓN	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Identificar a través de los medios o técnicas pertinentes cualquier incidente, y notificarlo al personal de recuperación y continuidad	❑	
Solicitar al Gerente de Proyectos & Tecnología las cintas de backup que se corresponden con el tiempo de ruptura o interrupción	❑	
Proceder a restaurar el backup,	❑	
Realizar un análisis de integridad del backup restaurado	❑	
Indicar cuando las operaciones pueden continuar	❑	
Retornar las cintas y otros materiales utilizados durante el proceso de recuperación	❑	
Proveer un informe de lo sucedido al personal de recuperación y continuidad	❑	
Participar del mantenimiento del plan de recuperación y aportar sugerencias para mejorar el mismo	❑	

Equipo de software

ACCIÓN A REALIZAR ANTES DEL INCIDENTE	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Ofrecer soporte a las aplicaciones de la empresa (SAP, Eikon, Exchange, Sistema operativo, etc.)	❑	
Instalar / Actualizar los sistemas y aplicaciones	❑	
Mantener copias de respaldo de las aplicaciones con sus actualizaciones	❑	
Realizar las pruebas y mantenimientos acorde a los esquemas establecidos	❑	
ACCIÓN DE RECUPERACIÓN	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Identificar a través de los medios o técnicas pertinentes cualquier incidente, y notificarlo al personal de recuperación y continuidad	❑	
Realizar las correcciones de software y o base de datos que sean requeridos, basado en las estrategias de recuperación.	❑	
Realizar un análisis de factibilidad de la solución aplicada	❑	
Indicar cuando las operaciones pueden continuar	❑	
Proveer un informe de lo sucedido al personal de recuperación y continuidad	❑	
Participar del mantenimiento del plan de recuperación y aportar sugerencias para mejorar el mismo	❑	

Equipo de recuperación de red.

ACCIÓN A REALIZAR ANTES DEL INCIDENTE	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Ofrecer soporte en lo relacionado a la red (conexiones, puntos de acceso, routers, switches, etc.)	❑	
Realizar el mantenimiento correspondiente a la red	❑	
Mantener actualizado el mapa de configuración de la red	❑	
Realizar las pruebas y mantenimientos acorde a los esquemas establecidos	❑	
ACCIÓN DE RECUPERACIÓN	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Identificar a través de los medios o técnicas pertinentes cualquier incidente, y notificarlo al personal de recuperación y continuidad	❑	
Solucionar el inconveniente que impacta la conectividad de la red, basado en las estrategias de recuperación	❑	
Realizar un análisis de factibilidad de la solución aplicada	❑	
Indicar cuando las operaciones pueden continuar	❑	
Proveer un informe de lo sucedido al personal de recuperación y continuidad	❑	
Participar del mantenimiento del plan de recuperación y aportar sugerencias para mejorar el mismo	❑	

Equipo de Comunicaciones

ACCIÓN A REALIZAR ANTES DEL INCIDENTE	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Ofrecer soporte en lo relacionado a las redes de comunicación de la empresa	❑	
Realizar el mantenimiento correspondiente de las redes de comunicación, incluyendo equipos y centrales	❑	
Mantener actualizado el mapa de configuración de la red de comunicación	❑	
Realizar las pruebas y mantenimientos acorde a los esquemas establecidos	❑	
ACCIÓN DE RECUPERACIÓN	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Identificar a través de los medios o técnicas pertinentes cualquier incidente, y notificarlo al personal de recuperación y continuidad	❑	
Aplicar una solución que permita solucionar el inconveniente ocurrido, basado en las estrategias de recuperación	❑	
Realizar un análisis de factibilidad de la solución aplicada	❑	
Indicar cuando las operaciones pueden continuar	❑	
Proveer un informe de lo sucedido al personal de recuperación y continuidad	❑	
Participar del mantenimiento del plan de recuperación y aportar sugerencias para mejorar el mismo	❑	

Equipo de software

ACCIÓN A REALIZAR ANTES DEL INCIDENTE	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Ofrecer soporte con el hardware de la empresa, (estaciones de trabajo, impresoras, servidores, rack)	❑	
Instalar / Actualizar cualquier hardware dentro de la empresa	❑	
Mantener actualizado el mapa de la disposición de equipos	❑	
Realizar el inventario de los activos del área de TI		
Realizar las pruebas y mantenimientos acorde a los esquemas establecidos	❑	
ACCIÓN DE RECUPERACIÓN	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Identificar a través de los medios o técnicas pertinentes cualquier incidente, y notificarlo al personal de recuperación y continuidad	❑	
Aplicar la optima solución que logre detener la interrupción basado en las estrategias de recuperación	❑	
Realizar un análisis de factibilidad de la solución aplicada	❑	
Indicar cuando las operaciones pueden continuar	❑	
Proveer un informe de lo sucedido al personal de recuperación y continuidad	❑	
Participar del mantenimiento del plan de recuperación y aportar sugerencias para mejorar el mismo	❑	

Actividades a ser realizadas por el equipo de gestión de continuidad.

ACCIÓN A REALIZAR ANTES DEL INCIDENTE	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Preparar el ambiente del Hot site, garantizando que sea una copia exacta del site original	❑	
Mantener actualizados los diagramas de disposición de equipos en el hot site.	❑	
Mantener actualizados los mapas de configuraciones estructurales (electricidad, comunicaciones)	❑	
Realizar el inventario de los activos del hot site		
Realizar las pruebas del hot site acorde al esquema establecido en el plan de pruebas del DRP	❑	
ACCIÓN DE RECUPERACIÓN	✓	**COMENTARIOS DE LA ACCIÓN REALIZADA**
Activar el Hot site (Ver proceso de activación en pág siguiente)	❑	
Comprobar buen funcionamiento de equipos y servidores	❑	
Realizar comprobación de data y aplicaciones	❑	
Realizar un análisis de factibilidad de la solución aplicada	❑	
Validar si es factible el cierre del hot site	❑	
Verificar estado de las bases de datos y servidores	❑	
Verificar estado de los equipos y aplicaciones	❑	
Proceder con el cierre del hot site	❑	
Realizar una evaluación de los costos de recuperación	❑	
Realizar un informe del incidente	❑	

Procedimiento de recuperación del área de TI ante desastres.

En este procedimiento colocaremos un listado de acciones a realizar durante el proceso de recuperación de un incidente de alto impacto, es decir un desastre en donde Quimidomsa se vea en la necesidad de recurrir a la utilización de las estrategias de recuperación seleccionadas.

Proceso de activación del Hot Site

El plan de recuperación desastres incluye un Hot Site suplente. El sitio cuenta con un sistema de copia de seguridad para el uso temporal mientras el sitio original está siendo restablecido. A continuación el procedimiento a seguir para la activación.

ACCIONES DE ACTIVACIÓN	✓
En caso de desastres notificar a los directivos la naturaleza del desastre y de la necesidad de activar el Hot Site.	❑
Solicitud de traslado de los equipos requeridos en el Hot Site, en caso necesario solicitarlo al director de continuidad.	❑
Confirmar por escrito el contenido de la notificación sea escrito o telefónico al director de continuidad y los directivos dentro de las 12 horas siguientes.	❑
Comience haciendo los arreglos de viaje necesarios para el sitio para el equipo de operaciones y el equipo de gestión de continuidad	❑
Confirme que todas las cintas necesarias están disponibles y empacadas para su envío a restaurar en el sistema de copia de seguridad.	❑
Preparar una orden de compra para cubrir la utilización de los equipos y otros medios que se utilicen durante el proceso.	❑
Revise la los checklist para todos los materiales necesarios antes de partir al Hot Site.	❑
Asegúrese de que el equipo de recuperación de desastres esté en el lugar de la catástrofe y que tenga la información necesaria para comenzar a restaurar el sitio.	❑
Prever los gastos de viaje (adelanto en efectivo).	❑
Después de llegar al Hot Site, comuníquese con la base de operaciones para establecer procedimientos de comunicaciones. (Se recomienda utilizar un punto donde puedan estar los directivos de la empresa reunidos que se conocerá como base de operaciones)	❑
Revisar los materiales llevados al Hot Site para la garantizar la integridad.	❑

Comienza la carga del sistema desde el servidor espejo.	❑
Compruebe la estabilidad del servidor espejo antes de cargar la data y procesos. (En caso de no realizarse una carga efectiva pueden cargar el sistema desde las cintas de backup guardadas).	❑
Actualizar directorio de direcciones IP y DNS internos utilizados por los procesos.	❑
Comience el normal funcionamiento en cuanto sea posible: 1. Operaciones diarias 2. Trabajos diarios 3. Trabajos semanales	❑
Planifique un horario de una copia de seguridad del sistema a fin de restablecer en un equipo de la sede principal cuando el sitio está disponible. (Utilice los procedimientos regulares de copia de seguridad del sistema).	❑
Asegure el sitio y distribuya las llaves según las necesidades.	❑
ACCIONES DE DESACTIVACIÓN	✓
Luego de restaurado el sistema o procesos del sitio original, se debe realizar una autorización por escrito firmada por el director de continuidad autorizando el cierre del hot site.	❑
Proceder a cargar el sistema en el site original, reasignando el directorio de direcciones IP y DNS internos que fueron actualizados con los datos del site original.	❑
Cargar en el sistema original las cintas de backup de las operaciones llevadas a cabo en el site alterno.	❑
Asegurar la integridad de la data almacenada en los backups antes de cerrar el hotsite	❑
Activar el sitio original	❑
Prepare los equipos de operaciones y el equipo de gestión de continuidad para el cierre de las aplicaciones en el hotsite	❑
Cerrar los sistemas y retornar funcionalidad de espejo	❑
Desalojar personal	❑
Asegure el sitio y retornar las llaves que fueron distribuidas.	❑

Proceso de reconstrucción del data center original.

El equipo de gestión debe evaluar los daños e iniciar la reconstrucción de un nuevo centro de cómputos en caso de que el original quede inoperable por completo.

Si el sitio original debe ser restaurado o sustituido, los siguientes son algunos de los factores a considerar:

- ¿Cuál es la disponibilidad proyectada de todo el equipo informático necesario?
- ¿Será más eficaz y eficiente para actualizar los sistemas informáticos con los nuevos equipos?
- ¿Cuál es el tiempo previsto para la reparación o construcción del centro?
- ¿Hay un lugar alternativo que más fácilmente pudiera ser acondicionado para los propósitos del centro de cómputo?

Una vez que la decisión de reconstruir el centro de cómputo se ha hecho, entonces debe seguir el siguiente esquema.

- Preparar la planta física del centro de cómputo.
- Determinar las necesidades de hardware actual y las posibles alternativas en caso de querer cambiar el inventario anterior.
- Condiciones del centro de cómputo, pies cuadrados, los requisitos de energía y requisitos de seguridad.
    - Diagrama del lugar
    - Requisitos de alimentación
    - Requisitos de seguridad: un área cerrada, preferiblemente con cerradura de combinación en una puerta.
    - Detectores o de alta temperatura, agua, humo, fuego y movimiento
    - Elevación del suelo.

Proceso para la restauración de los sistemas críticos

Luego de haber realizado la reparación o reconstrucción del sitio original, entonces es necesario restaurar el sistema. Antes de empezar: Encuentra las siguientes cintas, equipos, e información de la cámara de las cintas en el lugar o la ubicación de almacenamiento alterno:

- Si realiza la instalación desde el dispositivo de instalación alternativo, debe tener sus medios de cinta y los medios de CD-ROM que contiene la Licencia.
- Todas las cintas de la más reciente operación completa guardada.
- Las cintas de seguridad más recientes
- Las cintas de su configuración más recientes, si es necesario
- Todas las cintas que contienen los procesos diarios desde la más reciente operación.
- Cintas de los procesos diarios
- Cintas de los procesos semanales
- Cintas de los archivos almacenados a diario
- Historia de registro de la operación más reciente guardada completa
- Historia de registro de la operación semanal más reciente
- Los libros de la instalación del software, y manuales de los equipos en caso necesario
- Guía telefónica
- Kit de herramientas

Actividades y procedimientos ante desastres, crisis e incidentes.

Procedimiento de evacuación:

Lo más importante es la seguridad de los empleados. Es por esto que, en la mayoría de las situaciones de emergencia, evacuar el edificio es la medida de seguridad más efectiva. El proceso de evacuación propuesto para Quimidomsa establece lo siguiente:

ACCIONES E INDICACIONES DEL PROCESO DE EVACUACIÓN	✓
El empleado de contacto en emergencias de cada departamento tiene la facultad y la responsabilidad de avisar, tanto al Equipo de gestión de continuidad como al personal, para que se comience el evacuación cuando exista un riesgo que atente contra la seguridad debido a una situación de emergencia.	❑
Empleado de contacto en emergencias de cada departamento la activará y, a la misma vez, se comunicará con el Equipo de gestión de continuidad, quienes tendrán un megáfono, el cual se utilizará para alertar verbalmente a las personas sobre el evacuación. En las estructuras pequeñas donde no se requiere el uso de alarmas, el empleado de contacto en emergencias avisará al personal sobre el evacuación verbalmente o con el uso de un instrumento que emita un sonido de alerta (pito, bocina, etc.). El aviso verbal dirá repetidamente “ESTO ES UNA EMERGENCIA, FAVOR DE EVACUAR EL EDIFICIO AHORA”.	❑
Cuando se emita la señal de evacuación, todas las personas deben proceder inmediatamente a salir del edificio en forma ordenada. Una vez fuera, deben permanecer a, no menos de, 500 pies de distancia del edificio.	❑
La orden de evacuación es solamente para el área donde se da la señal. Si hay que evacuar el edificio completo, se impartirán instrucciones al respecto.	❑
La forma más rápida y efectiva de evacuar todo Quimidomsa es a pié. Por tal razón, se debe seguir este procedimiento a menos que se impartan otras instrucciones.	❑
Los empleados de contacto en emergencias de cada departamento identificarán con anticipación cualquier persona con impedimentos que utilice el edificio y que pueda tener dificultad para evacuarlo.	❑
Una vez notificada la situación, el equipo de gestión de continuidad tomará la decisión de activar este plan utilizando las guías establecidas.	❑

ACCIONES E INDICACIONES DEL PROCESO DE EVACUACIÓN (CONT)	✓
De ser necesario, el equipo de gestión de continuidad se comunicará con las entidades de Apoyo externo y los grupos directivos	❑
Luego de que pase la emergencia, el equipo de gestión de continuidad hará una evaluación del área y determinará si el edificio está en condiciones para ser retomado. Si hubiese la presencia de alguna entidad de Apoyo Externo, se tomará en consideración las sugerencias de estos en la toma de decisiones.	❑
El contacto en Emergencias le proveerá información al Equipo de gestión de continuidad, quienes harán un informe escrito sobre lo ocurrido. Una copia permanecerá en la Oficina del Coordinador de Emergencias, quien lo someterá al Director de Gestión de Continuidad con recomendaciones.	❑

Actividades durante un aviso de Tormentas y Huracanes:

Según las estadísticas, en el área del Caribe se forman aproximadamente diez (10) tormentas tropicales cada año, de las cuales seis (6) se convierten en huracanes. Todo esto durante los meses de junio a noviembre.

Con el propósito de reducir al mínimo los peligros y los daños a la propiedad y a las personas, se tomarán las siguientes precauciones:

Antes de la Temporada de Huracanes

El equipo de continuidad Ordenará la primera semana del mes de abril de cada año una Inspección de los terrenos y estructuras de Quimidomsa y se asegurará que estos estén libres de objetos que se puedan convertir en proyectiles o que obstruyan el paso del agua, con el objetivo de informar al director de continuidad y a los directivos sobre condiciones que deben ser mejoradas antes de que surja la emergencia.

ACCIONES E INDICACIONES ANTE AMENAZA DE HURACÁN O TORMENTA	✓
Tan pronto se emita un Boletín de Vigilancia de Tormenta o Huracán el director de continuidad se asegurará que todos los miembros del equipo de gestión de continuidad estén disponibles y conozcan su responsabilidad.	❑
El equipo de continuidad se asegurará que todas las instalaciones estén libres de basura, escombros y objetos que puedan ser arrastrados por el viento o que obstruyan el paso del agua.	❑
El equipo de continuidad ordenará que se aseguren todas las puertas y ventanas de todos los edificios.	❑
El equipo de continuidad se asegurará que se guarden aquellos objetos que no pueden ser removidos y que pueden presentar peligro.	❑
El director de continuidad deber informará a los directores de la empresa sobre las condiciones que no se hayan corregido, si alguna, que puedan ser mejoradas antes de la llegada de la tormenta o huracán.	❑
Bajo autorización de los directivos de la empresa y en caso necesario se declarará un receso de operaciones y ordenará que se detengan todas las labores que no tengan que ver con la preparación para la emergencia.	❑
Se despachará a todo el personal que no sea indispensable para las operaciones de emergencia.	❑
El equipo de continuidad se asegurarán que los archivos y escritorios estén lejos de las ventanas y que los papeles importantes se guarden en un lugar seguro.	❑
El equipo de continuidad desconectarán y asegurarán todo equipo sensitivo que se pueda dañar al mojarse.	❑
Los materiales y las sustancias químicas peligrosas se almacenarán en lugares apropiados. Éstos serán seleccionados previamente por el Director de continuidad	❑
Contener la tensión y mantener la calma durante el incidente	❑
Mantener comunicación con las autoridades locales	❑

Actividades ante derrames y emanaciones de Sustancias Peligrosas

Los derrames de algunas sustancias químicas pueden poner en peligro la vida, la salud y el ambiente. Algunos derrames se perciben a simple vista, otros son más difíciles de detectar. Por esto, se debe estar atentos a las siguientes señales: olores fuertes o fuera de lo normal, irritación en el sistema respiratorio, ojos o piel, niebla o vapores y sonido de silbido o siseo.

El mejor control que puede tener una empresa de productos químicos como el caso de Quimidomsa se obtiene a través de la prevención, planificando cada actividad y llevándola a cabo de una forma segura. Cada empleado del área de producción debe conocer los procedimientos de manejo de sustancias peligrosas, ya que de un modo u otro siempre tendrán la posibilidad de estar expuestos a estas.

Este procedimiento establece los pasos a seguir para atender los derrames o emanaciones de sustancias químicas que no se pudieron prevenir.

ACCIONES E INDICACIONES ANTES DE UN DERRAME O UNA EMANACIÓN DE UNA SUSTANCIA PELIGROSA	✓
Los supervisores de planta poseerán la lista actualizada de todas las sustancias químicas que se utilizan en su área de trabajo.	❑
Asegurar que todas las sustancias químicas tengan tapas, envases y etiquetas adecuadas.	❑
El equipo de continuidad se asegurará de tener en su área de trabajo los materiales y equipo de control de derrames (material absorbente, escoba, recogedor, bolsas de plástico resistentes, envases, etc.) de acuerdo con las clasificaciones de las sustancias químicas que poseen.	❑

ACCIONES DURANTE UN DERRAME O UNA EMANACIÓN DE UNA SUSTANCIA PELIGROSA	✓
El supervisor que evidencie el derrame deberá autorizar e indicar la evacuación inmediatamente del lugar a todas las personas que no son necesarias para atender el derrame.	❑
Identificar la sustancia a través de la etiqueta y se le informará al equipo de continuidad para que coordinen la limpieza.	❑
Verificar que el área es segura	❑
Controlar el derrame siempre y cuando no se ponga en riesgo la salud y seguridad de las personas.	❑
Abrir la mayor cantidad de puertas y ventanas para ventilar el lugar. Si el derrame se produce en un área con sistema de extracción de aire, se debe activar.	❑
Eliminar toda fuente de calor o ignición.	❑
Recoger los restos derramados utilizando equipo que no genere chispas, recoja los residuos cuando se haya absorbido todo el líquido derramado.	❑
Colocar los restos en las bolsas plásticas preparadas para esto o en algún otro envase adecuado (caja, botella, etc.)	❑
Rotular el envase como desperdicio peligroso	❑
Si se trata de la emanación de un gas: Si se trata de un gas que no es tóxico y el escape acaba de comenzar, intente controlar el mismo cerrando la válvula. Si se trata de un gas tóxico, y no se puede controlar al momento, desaloje el área inmediatamente	❑
De ser necesario, establecer comunicación con las entidades de Apoyo Externo	❑
Evaluar el peligro para determinar los efectos a la salud, propiedad y ambiente	❑
ACCIONES DESPUÉS UN DERRAME O UNA EMANACIÓN DE UNA SUSTANCIA PELIGROSA	✓
Los Supervisores a cargo de las instalaciones recopilarán toda la información relacionada con el derrame y las actividades realizadas para que el equipo de continuidad realice el informe final al director de continuidad.	❑
Evaluar si el área está en condiciones de ser retomada. Tomará en consideración las recomendaciones de las Entidades de Apoyo Externo presentes.	❑

Actividades ante Incendios

Los incendios son una de las emergencias más comunes en el ambiente laboral. Su magnitud puede ir desde un simple conato, fácilmente controlable, hasta un incendio de grandes proporciones. este Plan contempla que los empleados tratarán de controlar solamente fuegos pequeños que se puedan apagar con extintores de incendio portátiles u otros medios en los que han sido adiestrados.

Los incendios mayores a los antes descritos serán controlados por el Cuerpo de Bomberos en coordinación con el equipo de gestión de continuidad.

Durante emergencias de incendio la prioridad máxima es proteger la salud y la seguridad de todas las personas que se encuentran en el lugar. Para esto se seguirán los siguientes pasos:

ACCIONES ANTE UN INCENDIO	✓
La responsabilidad de activar este Plan está en manos de cualquier persona que vea o tenga conocimiento de que se ha desarrollado un incendio.	❑
Esta persona activará la alarma y avisará a cualquier empleado de la situación.	❑
El empleado deberá avisar inmediatamente al encargado de gestión del departamento o área donde se produjo el incidente.	❑
Intentar extinguir el incendio solamente cuando tengan certeza de poder hacerlo usando extintores portátiles u otros medios en los cuales han sido adiestrados.	❑
Si el incendio no es controlable, Iniciar proceso de evacuación	❑
El equipo de continuidad deberá comunicarse con los Bomberos	❑
El equipo de Emergencias de Quimidomsa asumirá la dirección y el control de las operaciones de control del incendio hasta la llegada de los bomberos.	❑

ACCIONES DESPUÉS DE UN INCENDIO	✓
Evaluación de daños y prepara los informes necesarios.	❑
Gestionar los recursos económicos necesarios para la recuperación de lo perdido	❑
Los supervisores, Directores de Departamentos y personal a cargo de las instalaciones serán los responsables de rendir informes de todo lo sucedido y de la actividad realizada	❑
El equipo de continuidad evaluará el proceso de respuesta a emergencias realizado y le hará un informe al director de continuidad	❑

Actividades ante amenaza de bombas y artefactos explosivos

Las amenazas de bombas y artefactos explosivos muchas veces son falsas. No obstante, siempre que ocurra una de éstas se tomarán las precauciones necesarias para proteger vidas, propiedad y el ambiente.

La mayoría de las amenazas se hacen por vía telefónica. Es por esto que se recomiendan los siguientes pasos a seguir:

ACCIONES AL RECIBIR UNA AMENAZA DE BOMBA O ARTEFACTOS EXPLOSIVOS	✓
La persona que reciba la llamada debe mantener la calma en todo momento. De esta manera la comunicación será más efectiva y se obtendrá más información.	❑
Hacer que la persona que llama permanezca en línea el mayor tiempo posible.	❑
Hacer que la persona que llama hable despacio y repita el mensaje.	❑
Hacer que la persona que llama le indique la localización de la bomba, la hora en que va a explotar o el sistema de detonación.	❑
Hacer que la persona que llama comprenda el peligro al que está exponiendo a las personas y a la propiedad de Quimidomsa.	❑
Tan pronto se corte la comunicación telefónica, reciba o encuentre una amenaza por escrito, se deberá llamar al equipo de continuidad.	❑

ACCIONES AL RECIBIR UNA AMENAZA DE BOMBA O ARTEFACTOS EXPLOSIVOS (CONT)	✓
El equipo de continuidad Inspeccionará y hará un registro de todo el edificio (interior y exterior) con la ayuda de, por lo menos, dos personas que trabajen en el área.	❑
Decidir si se desaloja el edificio o si se esperan los resultados de la inspección para tomar esta decisión.	❑
En caso de que se decida evacuar el edificio, seguir el proceso de evacuación	❑
Bajo ninguna circunstancia activar las alarmas de incendio en una amenaza de bombas o artefactos explosivos. Si fuera una bomba real, ésta se puede activar con la alarma.	❑

ACCIONES AL ENCONTRAR ARTEFACTOS SOSPECHOSOS	✓
El equipo de continuidad ordenará la evacuación de inmediato del edificio	❑
No tocar ni acercarse al objeto sospechoso.	❑
Remover del área todo material inflamable, siempre y cuando no se ponga en riesgo la vida de las personas.	❑
Contactar al escuadrón antibombas del ejército nacional	❑
Mantener vigilancia y control para que los empleados, y personal no autorizado permanezcan fuera del área.	❑
Esperar que el escuadrón antibombas controlen la situación.	❑

ACCIONES DESPUÉS DE UNA EMERGENCIA DE BOMBAS O ARTEFACTOS EXPLOSIVOS	✓
En caso de una explosión se debe realizar una evaluación de daños y los informes necesarios.	❑
Evaluar si es requerido activar el plan de continuidad para el área de TI y procurar el reinicio de las labores.	❑
Gestionar los recursos económicos necesarios para la recuperación de lo perdido	❑
El equipo de continuidad evaluará el proceso de respuesta a emergencias realizado y le hará un informe al director de continuidad	❑

Actividades ante Terremotos

República Dominicana está geográficamente ubicada en una zona muy susceptible a los terremotos. Éstos suceden sin previo aviso y tienen como peligro principal el derrumbamiento de edificios, incendios, entre otros. Dado este panorama, en Quimidomsa se seguirán estas guías:

ACCIONES AL MOMENTO DE OCURRIR UN TERREMOTO	✓
Conservar la calma	❑
De no lograr acceso al exterior, Protegerse bajo un escritorio o una mesa, acercarse al marco de alguna puerta, hacia una columna, permanecer en los pasillos	❑
Evitar correr	❑
Aléjese de los cristales.	❑
No utilizar velas, fósforos ni nada que produzca flamas durante o después del sismo.	❑
No utilizar los ascensores.	❑
Ayudar a cualquier persona que le solicite ayuda	❑

ACCIONES LUEGO DE HABER PASADO UN TERREMOTO	✓
Los encargados de continuidad de cada departamento deben avisar a los empleados para que se proceda con la evacuación inmediata del edificio	❑
Coordinar la inspección del edificio. En búsqueda de Personas atrapadas, heridas o lesionadas, Incendios, derrames de sustancias químicas, escapes de gas u otra situación que ponga en peligro la vida de los ocupantes.	❑
El equipo de continuidad Activará automáticamente este Plan.	❑
Movilizarse al Centro de Operaciones de Emergencia establecido en el momento	❑
Evaluar la información del estado de los edificios	❑

ACCIONES LUEGO DE HABER PASADO UN TERREMOTO (CONT)	✓
De ser necesario, establecer comunicación con las entidades de Apoyo Externo	❑
Hacer una evaluación del área y determinará si está en condiciones de ser retomada, si hubiese la presencia de entidades de Apoyo Externo, se tomará en cuenta sus recomendaciones.	❑
Evaluar si es requerido activar el plan de continuidad para el área de TI y procurar el reinicio de las labores.	❑
Gestionar los recursos económicos necesarios para la recuperación de lo perdido	❑
El equipo de continuidad evaluará el proceso de respuesta a emergencias realizado y le hará un informe al director de continuidad	❑

Actividades ante Inundaciones

Ante una inundación en Quimidomsa se seguirán los siguientes pasos:

ACCIONES ANTE EL AVISO DE INUNDACIONES	✓
Mantener al personal informado sobre la magnitud de la emergencia y el curso de acción que se seguirá.	❑
Los supervisores, y Directores de Departamentos o personal a cargo de las facilidades deberán guardar los documentos importantes en lugares seguros que no sean afectados por el agua.	❑
Coordinar el movimiento de equipo a lugares altos en su área o lo cubrirá con un material impermeable si el mismo no puede moverse.	❑
Remover y guardar en un lugar seguro el material o equipo que se encuentra en los patios o pasillos.	❑
Cerrar todas las válvulas de los servicios como gas, agua y fuentes que no sean imprescindibles.	❑
El equipo de continuidad debe inspeccionar todas las áreas	❑
Informar al director de gestión de continuidad sobre cualquier condición insegura que exista en Quimidomsa.	❑

ACCIONES ANTE EL AVISO DE INUNDACIONES (CONT)	✓
El equipo de TI debe asegurar que los documentos esenciales estén protegidos en bóvedas o con cualquier otro mecanismo.	❑
El área de TI debe estar cerrada herméticamente de manera que el agua no puede acceder a esta.	❑

ACCIONES ANTE INUNDACIONES SIN AVISO	✓
El equipo de continuidad activará este Plan y coordinará todas las actividades de respuesta a emergencias	❑
Obtener información sobre lo sucedido utilizando la información obtenida de las agencias de apoyo externo y de los medios noticiosos.	❑
Determinar la magnitud y el potencial de riesgo de la inundación.	❑
De ser necesario, coordinará las actividades de evacuación hacia áreas de refugio previamente establecidas	❑
De ser necesario, establecer comunicación con las entidades de apoyo externo	❑
Coordinar la prestación de servicios médicos y de primeros auxilios para el personal que lo necesite.	❑
Coordinar la adquisición de materiales y suministros necesarios para atender la emergencia.	❑
Seleccionar las rutas de entrada y salida	❑
El equipo de continuidad debe Informar al Comité de Emergencias sobre la situación y condiciones de las personas y el edificio e Informar al Grupo Directivo de cualquier situación que atente contra la vida o seguridad de las personas.	❑

ACCIONES DESPUÉS QUE OCURRA LA INUNDACIÓN	✓
Coordinar las labores de limpieza y desinfección para el control de plagas o epidemias en las áreas afectadas por la inundación.	❑
Evaluar las condiciones de Quimidomsa y determinar en cuáles áreas se pueden reanudar las labores.	❑
Coordinar una inspección para determinar las mejoras que se pueden realizar en los sistemas de drenaje y estructuras con el fin de prevenir emergencias futuras.	❑
Coordinar las labores de restauración de las áreas afectadas por la inundación.	❑
Supervisores, Directores de Departamento y Personal a cargo de las instalaciones deben realizar un inventario de todo el equipo y materiales a su cargo para determinar el estado y funcionamiento de los mismos.	❑

Actividades durante una falla en los sistemas:

Existen muchas razones por las que puede haber una falla en los sistemas, puede ser un ataque de un hacker, un virus, un error humano, una acción intencionada, una desconfiguración o por deterioro en los equipos.

Este plan contempla los pasos previos a realizarse antes de tomar la iniciativa de activar el plan de continuidad para el área de TI.

ACCIONES ANTE UNA FALLA EN LOS SISTEMAS	✓
El equipo de TI debe identificar la falla	❑
Realizar un análisis sobre el área afectada para determinar los daños producidos y cual fue la fuente que originó el problema.	❑
Tener a la mano las copias del software con sus licencias y los manuales de los equipos.	❑
Tener a la mano las más recientes cintas de respaldo en caso necesario	❑
Notificar al personal de continuidad sobre el incidente que se ha presentado y asegurase que estén presentes durante la corrección del incidente.	❑

ACCIONES ANTE UNA FALLA EN LOS SISTEMAS (CONT)	✓
Iniciar la corrección del problema: - Si es error de software, se debe reiniciar la aplicación y reintentar en caso negativo se procederá a reinstalar la aplicación y probar nuevamente. - Si es error de equipo, probar el encendido, comprobar sonidos o notificaciones diferentes al modo normal. - Si es ataque de Hacker, bloquear los puertos y enlaces de red, deshabilitar los accesos remotos, verificar estado del firewall, detener la ejecución de los procesos o sistemas que utilicen recursos de la red. - Si es un virus: Actualizar el antivirus y realizar una scan completo del sistema y detener los procesos que no sean de uso frecuente (desconocidos) - Etc.	❑
Si al realizar la corrección del problema se logró solucionar entonces, Evaluar las condiciones de Quimidomsa y determinar cuáles procesos no fueron afectados o atacados. En caso contrario entonces se debe activar plan de recuperación para el área de TI	❑
Controlar los daños: - Reinstalar los datos o procesos afectados desde las cintas de backup más recientes. - Notificar al fabricante del software el error ocurrido con su Log correspondiente. - Mantener un log de los últimos procesos ejecutados - Reparar los equipos afectados o comprar nuevo (Contactar suplidor) - Cambiar códigos de acceso, expirar contraseñas de todos los usuarios y cambiar direcciones de red fijas.	❑
-	

ACCIONES DESPUÉS DE UNA FALLA EN LOS SISTEMAS (CONT)	✓
Los supervisores, Directores de Departamentos y personal a cargo de las aplicaciones serán los responsables de reportar cualquier perdida de información o valor corrompido.	❑
El equipo de TI debe rendir informes de todo lo sucedido y o realizado.	❑
El equipo de continuidad evaluará el proceso de respuesta a emergencias realizado y le hará un informe al director de continuidad	❑

4.8 Procedimiento de activación del plan de recuperación del área de TI

Cuando cualquier área de la empresa identifica un incidente de alto riesgo o de riesgo extremo, deben pasar la información inmediatamente al equipo de gestión de continuidad, ya que es requerida la verificación y/o autorización de los directivos de la empresa así como del Director de Continuidad.

Luego de recibida la información, los directivos de la empresa en conjunto con el director de continuidad deben repasar la siguiente lista de actividades, dependiendo de esta lista de actividades se procede con la activación del plan, o si es posible utilizar las alternativas del plan de crisis e incidentes.

Lista de actividades del proceso de activación

1	**Verificar la situación: Determinar la magnitud del evento lo más rápido posible**
❑	Conozca los hechos. 1. ¿Cuál fue la fuente de la información? 2. ¿Qué tan creíble es la fuente de información? 3. ¿Fue la información obtenida de fuentes adicionales para poner en perspectiva el caso? 4. ¿La información es consistente con otras fuentes? 5. ¿Amerita este incidente que se active el plan? 6. ¿De ser necesario, la información fue aclarada a través de un experto en la información sometida?
2	**Realizar las notificaciones: Contactar e informar rápidamente a todos los que tengan que ver con este proceso dentro y fuera de la organización**
❑	• Personal clave dentro de la empresa (El equipo básico, de apoyo gerencial) • A todos los niveles de la organización que sean requeridos

	• A los proveedores locales y personal de emergencia • Los organismos estatales correspondientes • Otros grupos que puedan estar interesados (Directivos de la empresa que no estén presentes, clientes importantes, etc)
3	**Que hacer mientras trabajan en la recuperación del incidente: se debe organizar las asignaciones y verificar el cumplimiento de estas**
❑	1. ¿Todo el personal entiende su papel y sus tareas inmediatas? 2. ¿Se le asignaron labores específicas a cada miembro de los equipos? 3. ¿Han sido todos los expertos y portavoces bien informados? 4. ¿Ha sido todo el personal documentado y preparado el personal encargado en caso, en caso de ser abordado por los medios de comunicación?
4	**¿Qué hacer cuando ya la crisis está pasando? Monitorear los procesos de reanudación y hacer ajustes para la vida residual de la crisis.**
❑	• ¿Han sido los expertos, y personal externo actualizados con regularidad sobre el estado actual del incidente? • ¿Los medios de comunicación están controlados? • ¿Cuenta con todos los mecanismos para supervisar y evaluar la retroalimentación sobre los daños y causas del incidente?
5	**La crisis terminó, ahora es momento de analizar las causas y evaluar la situación desde un entorno de calma.**
❑	1. Analizar las informaciones y la fuente de procedencia 2. Evaluar la causa del incidente y determinar o asignar prioridades al plan de recuperación vigente que incluyan o mejoren la situación ocurrida 3. Capturar las opiniones del personal involucrado en la recuperación. 4. Actualizar el plan de recuperación

Capitulo 5: Diseño de Pruebas para el Plan de Recuperación de TI

5.1 Alcance y objetivos.

El óptimo funcionamiento del plan de recuperación de desastres dependerá en gran medida de las pruebas que se realicen de este, la robustez y efectivo del plan dependerán de cuantos escenarios abarque. Por tanto es recomendable realizar pruebas de cada uno de los diferentes incidentes que puedan presentarse tanto a lo interno como a lo externo de la organización.

Las situaciones deben irse intensificándose de manera gradual, iniciando en un evento o acción simple de realizar, hasta realizar las pruebas de aquellos procesos dentro del plan de recuperación que ameriten de un mayor esfuerzo.

Por tales motivos es requerido diseñar un esquema que debe ser seguido para la realización de las pruebas del plan de recuperación. Este plan no se crea, solo se diseña, es decir no hay que plantear listas, ni realizar análisis adicionales como en el plan de recuperación propio.

Alcance del plan de pruebas del DRP

El alcance de este plan es a todos los niveles de la empresa Quimidomsa, desde los niveles inferiores hasta la dirección de la empresa. Es requerido abarcar todos los niveles ya que el ambiente y cultura de continuidad deben prevalecer en la empresa y todos deben estar enfocados y preparados para cuando se presente una crisis.

Objetivos del plan de pruebas del DRP

Los objetivos del plan de pruebas del DRP para Quimidomsa son los siguientes:

- Validar que el DRP sea completo y funcional
- Evaluar los conocimientos y nivel de información del personal involucrado, identificando las zonas o el personal en el que luego se tendrá que reforzar

- Comprobar que los procedimientos y documentación estén actualizados
- Medir la habilidad y capacidad del lugar alterno
- Evaluar estado y cantidad de equipos y suministros en el lugar alterno
- Evaluar la capacidad de recuperación de los backups
- Evaluar el desempeño del personal involucrado
- Evaluar la coordinación entre los diferentes equipos que conforman el plan, fomentando el trabajo en equipo
- Cronometrar el tiempo de las actividades, para verificar el cumplimiento de los plazos acordados.
- En general, evaluar el desempeño de todos los procesos operativos y de los sistemas relacionados con el negocio.

5.2 Tipos de pruebas

Antes de realizar una prueba a algún proceso o área en particular, es requerido conocer el tipo de prueba adecuado para cada proceso, (En esta parte nos referimos a los procesos listados en las actividades del plan de recuperación).

- Pruebas de escrito o sobre papel

Es una reunión donde participan el personal de gestión de continuidad y el personal del área seleccionada. Consiste en plantear un escenario que represente riesgo a la empresa, para que el personal seleccionado aplique un razonamiento y evaluación sobre las acciones que corresponde tomar en cada parte del proceso. (Puede ser de todo o solo de una parte del plan).

- Pruebas de simulación o especificas

Es una representación de un escenario de contingencia donde participan los equipos de trabajo seleccionados, Puede ser evaluado todo el plan o solo la parte del plan que

corresponde al equipo de trabajo seleccionado. En algunos casos se puede realizar una acción concreta de desconexión o interrupción que impacte el área evaluada.

- Prueba total

Es donde se ponen a prueba todos los niveles de la compañía y es donde se identifican el eslabón más débil de toda la cadena de continuidad de la empresa. Consiste en realizar una interrupción programada para a partir de ese momento medir el proceso de recuperación y reanudación.

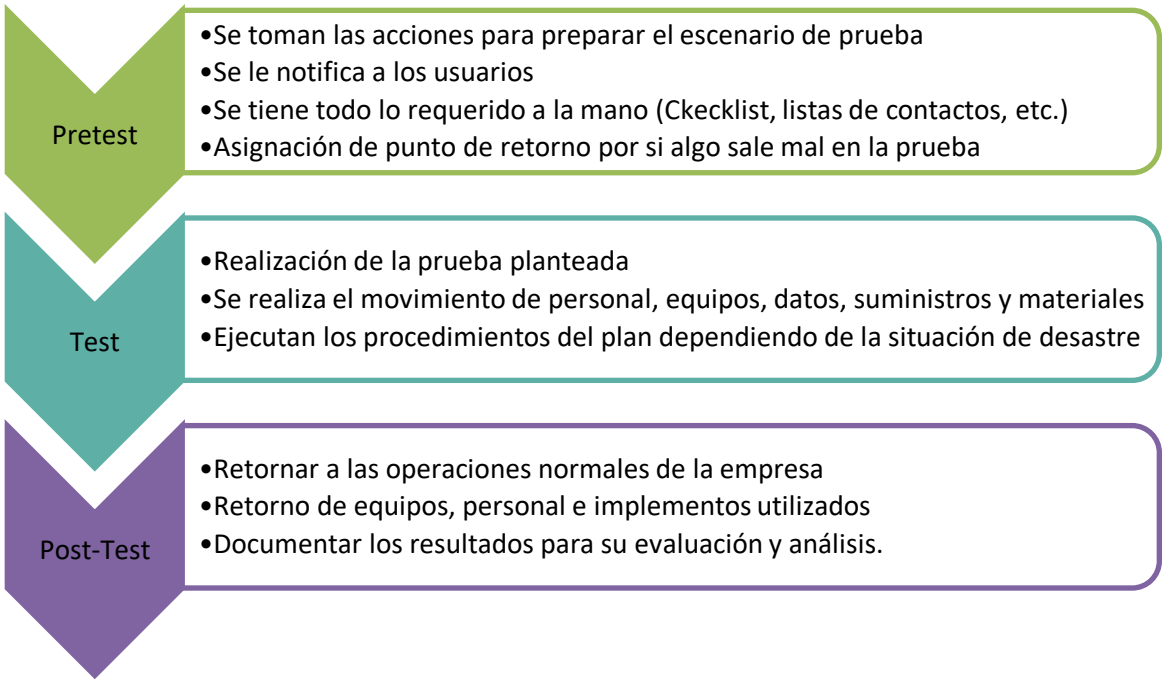
5.3 Escenarios y supuestos

Los escenarios y supuestos que se deben presentar, dependerán del tipo de prueba a realizar, pero en sentido general cada supuesto tendrá un objetivo en particular dependiendo del proceso verificado:

- Área Técnica - ¿Funcionan los equipos?
- Procedimientos - ¿Son correctos los procedimientos?
- Logística - ¿Los procedimientos presentan una secuencia lógica?
- Entrega a tiempo - ¿Consiguen los procedimientos cumplir con los RTO de cada actividad?
- Administrativo - ¿Son los procedimientos fáciles de gestionar?
- Personal - ¿Están involucradas las personas correctas? ¿Poseen las habilidades, autoridad y experiencia adecuadas?

La selección de la amenaza o incidente que será probado debe ser evaluada por el equipo de gestión de la continuidad y aprobada por el director de gestión de continuidad. Las amenazas seleccionadas bien pueden ser situaciones diferentes o no conocidas, como las que situaciones de emergencia que forman parte del plan de Crisis e Incidentes (Ver capitulo 4 para ver lista de actividades a realizar ante cada incidente).

La amenaza seleccionada (el escenario o supuesto) deben ser analizados por el equipo de gestión de continuidad previo a realizar la prueba, y luego de haber realizado la prueba deben analizar sus resultados. Es por esto que se hace referencia al siguiente esquema del proceso de aplicación de las pruebas del DRP:



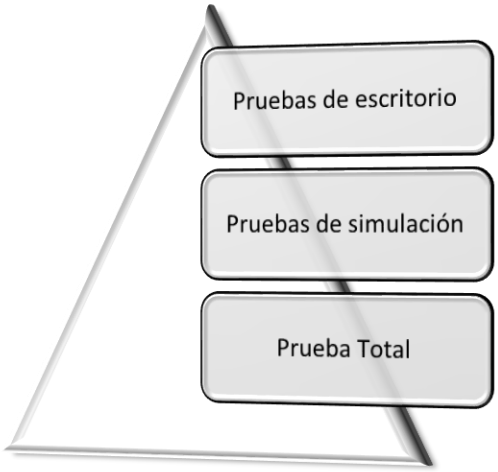
5.4 Cronograma de Pruebas

La periodicidad de las pruebas dependerá del grado de movilidad del plan, del tipo de prueba a realizar y de las condiciones de la compañía.

Nos referimos a lo siguiente:

Grado de movilidad: A la frecuencia de cambio organizacional, salida y entrada de personal, equipos, etc.

Tipo de prueba: Dentro de los tres tipos de prueba existe una distinción que va asociada al impacto que tendía una interrupción o una maniobra de prueba en el área de producción y a los costos operacionales intrínsecos.



La pirámide expresa la jerarquía existente, un tipo de prueba y otro, las pruebas de escritorio abarcan poco, sin embargo son más frecuentes ya que implican menos costos operativos y menor impacto en las operaciones de producción. Por el otro extremo se tienen las pruebas totales que si bien es cierto que son las más funcionales ya que abarcan toda la empresa, son las que infieren mayor gasto y producen un impacto mayor en el área de producción.

Cronograma

De lo anterior podemos sugerir el siguiente esquema con el siguiente formulario:

Frecuencia	Tipo de prueba	Áreas	Horario	Responsables
Mensual (Evaluando en el mes todas las áreas de la empresa)	De escritorio	Departamentos Seleccionados	Matutino	Equipo de gestión de TI
Bimensual	Simulación	Equipos de continuidad	Matutino / Vespertino	Equipo de gestión de TI / Responsables de equipos

		Seleccionados		
Semestral	Total	Todas las áreas	Nocturno	Equipo de gestión de TI / Responsables de equipos / Directores de la empresa

Anexo al formulario anterior debe estar el siguiente uno para cada tipo de prueba. Donde se colocan la fecha de la prueba, cualquier hallazgo que se haya realizado a favor o en contra del proceso, el área involucrada, la hora de inicio, la de fin, y algunas consideraciones a ser tomadas para la próxima prueba.

Fecha	Hallazgo	Áreas	Inicio	Fin	Consideraciones

Finalmente prueba debe estar asociada del siguiente formulario estilo checklist con la acción puesta a prueba, la evaluación positiva o negativa de la misma, y su comentario.

Acción o proceso	Si	No	Comentarios

5.5 Conclusión

Todo comentario o resultado de las pruebas debe servir de feedback para mejorar el plan, por tanto es necesario realizar una observación integra y objetiva de lo sucedido durante la realización de la prueba.

Los resultados y comentarios obtenidos del proceso de observación deben ser evaluados de manera cuantitativa, es decir con parámetros que nos arrojen valores porcentuales de lo sucedido.

Entre los parámetros más utilizados están:

- **Medición por cantidad:** Se mide la cantidad de trabajo realizado en la prueba. Usualmente aplicado en el análisis de pruebas totales donde se realizan muchos procesos, tanto en el site original como en el alterno.

- **Medición por Exactitud:** puede ser la exactitud de entrada de los datos en ambiente de recuperación en comparación al ambiente normal. O la exactitud de los ciclos de procesamiento, querys, etc, del ambiente de recuperación en contraposición al ambiente normal.
- **Medición por conteo:** Donde se cuenta el número de procesos críticos que lograron ser recuperados con cada una de sus transacciones. Al igual se evalúa la cantidad de suministros, listas, procedimientos y demás que son requeridos contra lo que realmente fue utilizado en la prueba.
- **Medición por tiempo:** Mide el tiempo transcurrido para realizar cada acción o proceso, en contraste con el tiempo de recuperación establecido para el mismo.

Capitulo 6: Mantenimiento Del Plan de recuperación de TI

6.1 Aplicación del plan de mantenimiento

Los cambios en las organizaciones se producen todo el tiempo. Un ejemplo de estos son los Productos y servicios cambian al igual que su método de entrega.

El aumento de los procesos tecnológicos basados en los últimos diez años, y en particular en los últimos cinco años, han aumentado significativamente el nivel de dependencia de la disponibilidad de los sistemas y la información para que el negocio funcione con eficacia. Estos cambios son probablemente continuos, y es probable que la única certeza es que el ritmo de cambio siga aumentando.

Para garantizar esto, todas las actualizaciones que afectan al plan de recuperación de desastres deben estar debidamente estructuradas y controladas. Además, cada vez que se realizan cambios en el plan deben ser completamente probado, y los cambios adecuados deben tomarse en cuenta para los materiales de formación. Esto implicará el uso de los procedimientos formales de control de cambios bajo el control del propietario del plan.

El mantenimiento del plan es un proceso sencillo. Se comienza con una revisión del plan existente y se examina en su totalidad, realizando cambios a cualquier información que pueda haber variado. En ese instante, se debe volver a evaluar los sistemas de aplicación y determinar cuáles son los más importantes para la organización. Las modificaciones a esta parte del plan causarán modificaciones consecutivas a los procedimientos de recuperación. Sin embargo, esto no debería verse como un problema porque probablemente la sección de procedimientos tenga que actualizarse de todas formas debido a otros cambios. Si se han realizado modificaciones al sistema de copias

de seguridad, hay que cerciorarse de incluir la información sobre el funcionamiento del nuevo o actualizado sistema.

6.2 Periodicidad de los mantenimientos

El mantenimiento del plan se recomienda realizarse Trimestralmente debido a los cambios constantes que puede afectar la continuidad del negocio. Dicha Gestión de Continuidad del Negocio de los coordinadores del equipo asegura que el Plan se somete a una revisión más formal para confirmar la incorporación de todos los cambios desde el trimestre anterior.

Se recomienda además que anualmente, el negocio de Gestión de la Continuidad de los coordinadores del equipo inicie una revisión completa del Plan, lo que podría dar lugar a importantes revisiones a este documento. Estas revisiones se distribuirán a todo el personal autorizado, que intercambian sus planes de edad para los planes recientemente revisado. En ese momento los coordinadores proporcionarán un informe de situación anual sobre planificación de la continuidad de la Administración de Informática del Comité Directivo.

6.3 Asignación de responsabilidades para el soporte y mantenimiento

Recomendamos que esta tarea de gestión y realización del mantenimiento del plan este a cargo del equipo de sistemas y soporte TI conjunto con la dirección de gestión de continuidad. El propósito de elegir a estos equipos como responsables se debe a que estos equipos son los más importantes en todo el proceso de recuperación ya que son los que mantienen el flujo de las operaciones en su curso normal.

Estos responsables mantendrán el control general de la continuidad del negocio pero cada responsable de una unidad de negocio deberá mantener las secciones de la continuidad de negocios correspondientes a sus áreas actualizadas todo el tiempo.

Es importante que los responsables del plan de mantenimiento y del Equipo de recuperación del negocio estén totalmente informados de todo cambio aprobado del plan.

Evento	Solicitante	Responsable	Descripción	Fecha realizada	Horario
Cambios en SAP Productivo					
Cambios de RED					
Cambios de autorización					
..					

6.4 Revisión y evaluación del mantenimiento

Los planes deben ser actualizados para mantener listas precisas de personal clave, número de teléfono, árboles de llamadas y elementos del plan que puedan verse afectados por cambios en la estructura de unidades o funciones. El respectivo Jefe de Departamento y Director, Decano o Vice Canciller (o designado vicerrector o el vice canciller de asociación) y la cohorte de Coordinador de revisión debe y aprobar el plan actualizado de, al menos, una periodicidad anual.

Objetivo del mantenimiento se debe a la revisión constante de los procesos. A continuación les mostramos algunas sugerencias:

•Revisar y cuestionar las suposiciones hechas en el Análisis del Impacto en el Negocio acerca del entorno en el que opera la organización para determinar si los imperativos de tiempo han cambiado desde la última revisión.

•Revisar la idoneidad y disponibilidad de aquellos servicios externos que podrían ser exigidos por una organización en momentos difíciles, como la restauración de activos, ubicaciones de recuperación y Subcontrataciones

•Revisar los planes de Continuidad de Negocio para proveedores de componentes cuya entrega a tiempo es crítica para el negocio

•Evaluar si los cambios y enmiendas crean una necesidad de formación, concienciación y/o Comunicación.

6.5 Validación de posibles actualizaciones

Para completar y realizar actualizaciones necesarias encontradas en el mantenimiento, se recomienda un proceso de validación por la dirección de gestión de continuidad donde estos estarán encargados de velar por el buen funcionamiento de la continuidad de negocios. Este proceso de validación se debe llevar rigurosamente, donde se crea un documento interno definiendo la actualización a realizar, además con los departamentos afectados y el grado de criticidad para la empresas. Este documento deberá ser firmado y sellado aceptando la realización de las actualizaciones. A continuación un ejemplo del documento interno para la realización de actualizaciones.

Validación de Actualizaciones

Fecha: _____ Área afectada: _____

Solicitante: _____ Referencia: _____

Descripción de Actualización	Código Actualización	Sistema afectado	Horario	Duración	Nivel de Criticidad

Director Continuidad: _____ Gerente de Tecnología: _____

Recibido el: _____

Documentación Interna

Capitulo 7: Plan de manejo y comunicación ante crisis e incidentes

7.1 Objetivo

Una situación que afecta de forma relevante y negativa las empresas tiende a afectar su imagen. Los expertos dan como un hecho que el desarrollo y supervivencia de una empresa está determinada por la imagen que proyecta hacia el exterior y el interior. Para gestionar y lograr una valoración positiva del negocio es recomendable la puesta en marcha de un plan de comunicación.

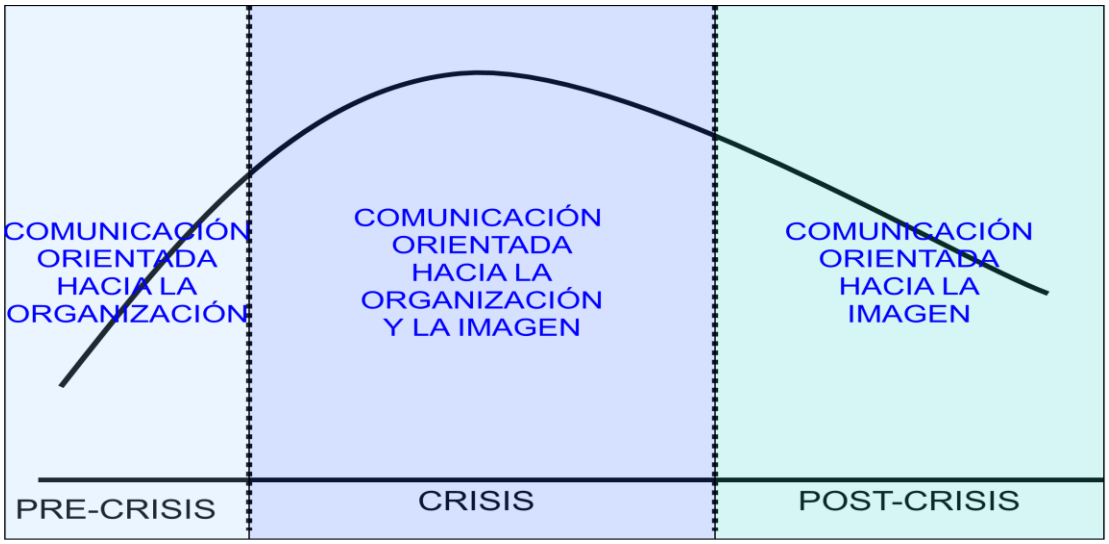
La principal finalidad de un plan de comunicación es determinar y proyectar la imagen deseada, aquella que nos interesa trasmitir a todos los destinatarios aún en tiempos de crisis.

Una correcta gestión del plan de comunicación provee a la empresa de un importante valor agregado de cara al mercado e incluso como retención de talentos y un mayor compromiso del personal.

El plan de comunicación es una guía normativa que determina las pautas de comportamiento corporativo ante una emergencia y establece los principios generales de la gestión de la crisis. Con este plan aplicado para la empresa Quimidomsa se pretende potenciar la imagen corporativa en todos los niveles, apoyar la labor de los departamentos de ventas y marketing y proyectar un clima favorable hacia los productos que oferta. .

7.2 Etapas de manejo de incidentes

Durante un incidente o crisis se identifica el siguiente ciclo:



Donde la línea expresa el tipo de comunicación que se dá durante un incidente.

Las siguientes son las fases o etapas que se atraviesan con el el plan de comunicación

1. Determinar qué queremos conseguir, cuáles son nuestros objetivos
2. Decidir a quién vamos a dirigir nuestra comunicación o información
3. Pensar cuál es la idea que queremos transmitir
4. Fijar el presupuesto con el que contamos (En caso de utilizar algún medio publicitario)
5. Seleccionar los medios apropiados y su frecuencia de utilización

La estructura de un plan de comunicación es determinante para asegurar unas bases sólidas, así que en síntesis, el plan de comunicación debe pasar por una primera fase de análisis, recogida de datos y evaluación de los mismos. Posteriormente, hay que establecer los objetivos primordiales y las actividades que deben realizarse para lograrlos, así como el tiempo estimado y el presupuesto necesario para ponerlo en práctica. Tras su puesta en marcha, sólo nos queda realizar un seguimiento continuo de los resultados.

7.3 Plan de manejo de crisis

Algunas normas generales de prevención que se proponen para situaciones de crisis son:

- Brochures de información general acerca de la compañía. (Para repartir a los clientes que se acercan así como aquellos que están perdiendo interés en la compañía)
- Antecedentes de crisis, especialmente dentro del mismo sector de actividad, para estar documentado y poder realizar una relación comparativa del escenario actual de la empresa y hacer referencia a dicho antecedente.
- Casos simulados de crisis con las soluciones formalizadas.
- Un directorio de periodistas especializados en el campo de acción de la química.

Recomendaciones:

Para abordar un momento de crisis de forma efectiva, es necesario seguir los siguientes procesos

- Recopilar toda la información posible del estado de la empresa
- Analizar dichas informaciones y cuantificar su valor
- Nunca mentir sobre la información crucial ni ocultar datos para minimizar la situación.
- No precipitarse por la presión de los periodistas u otros grupos.
- Evitar las lagunas de información, comunicando con rapidez.

- Comprobar el alcance de la crisis.
- Determinar la secuencia y la coherencia de la comunicación.
- Crear un plan de acción para el relanzamiento de la imagen corporativa.

Principios estratégicos:

- **Estrategia de anticipación**: que exige disponer de un plan anticrisis y una actitud por parte de la empresa de prevención.
- **Estrategia del silencio:** se trata de no reaccionar o hablar lo menos posible. Se utiliza especialmente en casos de rumores infundados ayudan a poder ser extinguirlos (se agotan por falta de respuesta)
- **Estrategia de Agilidad**, es decir, una vez declarada la crisis, la respuesta a la misma debe ser inmediata. Las primeras veinticuatro horas suelen ser cruciales
- **Estrategia de la negación:** niega el incidente acontecido, rechazando el interés del tema.
- **Estrategia de transferencia de responsabilidades:** culpar de la responsailidad a un tercero. (Eficaz a corto plazo para ganar tiempo.)
- **La veracidad**, es otro, de los principios incuestionables de la comunicación corporativa y de crisis, en la cual se explica, el hecho de reservar determinada información en momentos determinados.

El plan de comunicación de crisis es para utilizarlo durante y después de un desastre. Debe detallarse cómo la empresa se comunicará con los empleados, autoridades locales, clientes y otros durante y después de un desastre.

1. Empleados: Esté preparado para proporcionar a los empleados información sobre cuándo, si y cómo presentarse a trabajar tras una emergencia.

Para esto se debe establecer una red de comunicación telefónica, una alerta por correo electrónico o una grabación telefónica para comunicarse con los empleados.

2. Gerencia: Se debe proporcionar a los ejecutivos superiores de la compañía toda la información pertinente y que sea necesaria para la protección de empleados, clientes, vendedores e instalaciones cercanas.

3. Público: Es importante mantener informado al público en general acerca de que se están utilizando todos los recursos para proteger a los trabajadores y a la comunidad. También es importante comunicar que existen planes de recuperación de las actividades de la compañía.

4. Clientes: Se debe mantener actualizados a los clientes sobre cuándo se recibirán productos y se reanudarán los servicios, en los casos que corresponda.

5. Gobierno: Informar a las autoridades sobre las acciones que la compañía está preparada para hacer con el fin de ayudar en el esfuerzo de recuperación. Se debe comunicar también con las autoridades locales.

7.4 Mantenimiento del plan de comunicación

Elaborar e implantar un excelente plan de comunicación en la empresa, es solo el primer paso, partir de este momento, se debe velar para que el proyecto se vaya adaptando a los sucesivos cambios y sea siempre igual de efectivo.

Para que este plan de comunicación sea eficiente aún con el paso del tiempo, es imprescindible llevar a cabo una gestión que incluya las siguientes actividades básicas:

-Creación y mantenimiento de una política de comunicación interna, coherente, compatible y complementaria con la actual política de recursos humanos de la pyme.

-Sensibilizar a todos los empleados sobre la importancia que la comunicación, en este caso la interna, tiene en la empresa, involucrándola en el desarrollo de las diferentes etapas que requiera el proyecto.

-Garantizar siempre un plan que mejore de forma sustancial los flujos de comunicación, que sea capaz de crear nuevos canales, y amplíe y optimice los ya existentes.

-Llevar a cabo de forma periódica los diagnósticos necesarios para identificar cuáles son las fortalezas, oportunidades, debilidades y amenazas que forman el clima organizacional de la empresa

-Elaborar y potenciar todo tipo de mecanismos de participación que faciliten que cada persona desde su rol con la empresa, pueda realizar aportes positivos para la ejecución efectiva del plan.

-Incentivar el uso de los distintos medios de comunicación que existen en la empresa, como Intranet o los boletines internos. A nivel externo, hay que intentar tener la máxima presencia en los canales convencionales de información.

Capitulo 8: Programa de Capacitación, Concientización y Difusión

Capitulo 8 Programa de Capacitación, concientización y Difusión

La columna vertebral de organización de la planificación de continuidad de negocio es el equipo de administración de la Continuidad del Negocio. En el caso de una catástrofe que afecte la organización, el Equipo de Gestión de Continuidad de Negocio responderá de conformidad con este Plan y pondrá en marcha acciones específicas para la recuperación. El Equipo de Gestión de Continuidad de Negocio se llama a la acción bajo la autoridad de la Administración de Informática del Comité Directivo que tiene la responsabilidad de autorizar las acciones respecto de Planificación de Continuidad de Negocio. Por este motivo es importante y necesario capacitar al personal implicado para la realización eficiente del plan.

En este capítulo se presentara el desarrollo un plan de capacitación y de promoción de conciencia que es apropiado para las necesidades específicas de Quimidomsa. Los servicios varían de sesiones de capacitación para personal clave a técnicas innovadoras para asegurar que todos los empleados estén listos a responder y sepan seguir el protocolo de un plan después de cualquier tipo de interrupción.

El objetivo de la capacitación es:

"Entrenar al personal en los procedimientos particulares a seguir durante el proceso de recuperación del negocio".

Y el alcance de la capacitación es:

"La capacitación debe llevarse a cabo de manera detallada y exhaustiva para que el personal se familiarice con todos los aspectos del proceso de recuperación. La

capacitación cubre todos los aspectos de la sección de actividades de recuperación del negocio del BCP incluyendo la recuperación de los sistemas de IT".

8.1 Definición de la audiencia y la logística.

En el mismo orden de la implementación del plan, los equipos formados se utilizaran con el mismo esquema para la creación de los niveles de capacitación y la audiencia. A continuación les detallamos los equipos que serán capacitados:

- **Gerenciales**
    - Equipo de soportes, datos y registros.
    - Equipo de trámites Legales.
    - Equipo de Recuperación
    - Equipo de coordinación de medios y prensa

- **Recursos Humanos**
    - Equipo de operaciones de emergencia y salvamento.
    - Equipo de seguridad.
    - Equipo de coordinación y reubicación.

- **Sistemas y soporte TI**
    - Equipo de almacenamiento y respaldo.
    - Equipo de software.
    - Equipo de recuperación de red.
    - Equipo de Comunicaciones.
    - Equipo de Hardware.

Para dicha realización hemos diseñado diferentes niveles de capacitación para los grupos nombrados anteriormente. Esto con la finalidad de suplir conocimiento necesario

para la realización del plan de recuperación de desastre (DRP) de acuerdo al rol establecido.

La responsabilidad de la gestión e impartición de todas la capacitación y concientización al personal lo tendrá el departamento de Recursos humanos conjunto a la dirección de gestión de continuidad, donde garantizaran la seguridad y conocimiento al empleado para la realización del plan.

Las capacitaciones son de manera jerárquica y comienza con un curso de inducción al nuevo personal y luego a cada grupo en específico.

Una vez organizada la capacitación a los empleados, se comunicara la agenda de los programas que se acordaron. Se enviara una comunicación por separado a los gerentes de las unidades de negocio avisando sobre las fechas de capacitación establecidas para su personal. Se le dará información a cada miembro del personal sobre su rol y sus responsabilidades en caso de emergencia.

Cada capacitación estará documentada, y esta servirá a la hora de algún cambio de personal a otro nivel de capacitación, a estos se le entregara copia de dichas capacitaciones para documentarse hasta que la capacitación presencial sea realizada.

Las capacitaciones será revisada y de nuevo impartida en respuesta a cambios en:

•Las actividades de negocio que afectan a las prioridades de la Continuidad del negocio

•La legislación que afecta a las necesidades de la continuidad del negocio

•Los riesgos para la continuidad de negocios, entre ellos las amenazas y vulnerabilidades a la seguridad y otros riesgos relacionados con el negocio

•Los requisitos de la empresa y clientes o socios relativos a la disponibilidad de información y servicios, donde afecta el plan actual de Recuperación de desastre.
Esta revisión se hará periódicamente para asegurar de que cada cambio realizado en cualquier unidad de negocio fuese modificado previamente en el plan de recuperación e informado a las demás áreas posiblemente afectadas.

Los programas individuales de capacitación y todos los procesos generales de capacitación del Plan de recuperación de Desastre (DRP) serán evaluados luego de impartir la capacitación para asegurar que sean efectivos y aplicables. Esta información será distribuida entre los capacitadores y los asistentes para que completen los cuestionarios de feedback.

8.2 Programa de capacitación del DRP.

De acuerdo al planteamiento anterior, y tomando en consideración los distintos grupos para capacitar, se crearon nivel de Capacitación para satisfacer las demandas de cada uno de los grupos. Estos niveles son específicos para cada grupo en particular, excepto uno que es para todo el personal. A continuación se detalla los niveles y el periodo para su realización.

Nivel	Audiencia	Recurrencia	Objetivo
Primer Nivel	Nuevo personal	Una vez	Inducción del personal. Importancia de la continuidad de negocios. Rol que ocupa en el plan de recuperación.
Segundo Nivel	Gerenciales	Anual	Importancia de la Continuidad de negocios. Mostrar vulnerabilidades y controles. Consecuencias financieras. Herramientas para contrarrestar Desastres.
Tercer Nivel	Recursos Humanos	Semestral	Importancia de la Continuidad de negocios. Controles de seguridad. Conocimientos de Primeros auxilios. Procedimientos de emergencias. Procedimiento de reubicación.
Cuarto Nivel	Sistemas y Soporte TI	Semestral	Importancia de la Continuidad de negocios. Mejoras y controles a utilizar. Seguridad en la Red. Herramientas para contrarrestar Desastres.

8.3 Programa de Concientización

La instauración de una Continuidad de Negocio dentro de la cultura de la organización dependerá de su integración con la gestión diaria y estratégica de la organización y su correspondencia con las prioridades del negocio. Una cultura de continuidad de negocios garantizará que una organización puede:

•Desarrollar un programa de continuidad de negocios de forma más eficiente

•Inculcar confianza en personal y clientes en su capacidad para sobrellevar los trastornos

•Mejorar su robustez con el paso del tiempo al asegurarse de que todas las decisiones en todos los Niveles toman en cuenta las implicaciones para la continuidad de negocios.

•Minimizar el impacto y la probabilidad de los trastornos

8.4 Programa de difusión

Para lograr estos objetivos se requiere una ardua labor en concientizar a todo el personal de incluir la continuidad de negocio en la cultura de la empresa. Por ello, se utilizara varias herramientas para llevar a cabo este objetivo. A continuaciones recomendamos las siguientes actividades a realizar para la concientización y difusión de la continuidad de negocios al personal.

- Videos.
- Fondos de pantallas.
- Publicaciones de casos de éxitos.
- Conferencias y seminarios con profesionales de la continuidad de negocios (Impartidos dentro y fuera de la organización)
- E-learning.
- Documentos informativos (Físicos y en Intranet)

- Revistas corporativas, boletines, artículos en la revista de la empresa
- Visitas a los emplazamientos de reinicio de actividades y centros de gestión de incidentes.

Conclusión

Los cambios positivos que traen consigo la continuidad del negocio, crean un ambiente de estabilidad y confianza tanto para clientes como para los empleados y dueños de la empresa. Al implementar el plan de recuperación la comunicación de la empresa y las relaciones interdepartamentales se afianzan, creando un ambiente unión que soporta los objetivos y metas de la compañía.

En el caso de Quimidomsa es se pasó de ser reactivo a proactivo, aprendiendo a realizar las acciones correctivas cuando sea necesario, los empleados aprendieron que actuar con responsabilidad también ayuda a disminuir el riesgo. Con el plan propuesto la compañía podrá fácilmente ofrecer una respuesta ordenada ante un desastre.

Finalmente se comprende que la continuidad de los servicios es una labor de todos los empleados, y en la que cada uno juega un papel vital.

Bibliografía

Manuales y libros electrónicos

Manual de mejores prácticas de continuidad
http://www.thebci.org/

Manual de seguridad Informática
www.piramidedigital.com/Documentos/ICT/pdictsegurindadinformaticariesgos.pdf

Ciclo de vida de BCM
http://www.scribd.com/doc/24765645/BCM-Lifecycle

Referencias y publicaciones electrónicas

"Business Continuity Plan Development."
www.continuitycentral.com

"The Business Case for Disaster Recovery Planning: Calculating the Cost of Downtime."
www.ironmountain.com

"The Future of Business Continuity."
www.psgroup.com

"DRP y BCP: Continuidad Operativa"
www.gcpglobal.com

Instituciones

Disaster Recovery Institute International (DRII)
http://www.drii.org/

Business Continuity Insights (BCI)
http://www.thebci.org/

Asociación Dominicana de Mitigación de desastres
www.**desastre**.org/

Apéndices

Apéndice I

1. Selección del título y definición del tema.

Plan de Recuperación de Desastres (DRP) para el área de TI, Caso: empresa Quimidomsa.

2. Planteamiento del problema.

El auge de la tecnología de información en los negocios ha encadenado una dependencia casi total de los sistemas de información en la mayoría de los procesos y actividades de las organizaciones. Por este motivo, las organizaciones requieren de sus sistemas, datos y sus informaciones relevantes puedan ser preservados, aunque no todas las organizaciones han implementado un plan que le provea la capacidad para restablecer las operaciones de TI y de negocio, ante eventos que pudieran interrumpir el cumplimiento de lograr sus objetivos estratégicos.

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

Por esta dependencia de TI, cualquier falla podría causar serias pérdidas financieras y poner en peligro la supervivencia de cualquier organización. Para contrarrestar cualquier amenaza debemos contar con un adecuado plan que reduzca el tiempo de interrupción

de los servicios de TI y garantice la recuperación el flujo de información de la organización.

3. Objetivos de la investigación.

a. Objetivo general.

Diseñar e implementar un plan de recuperación de desastre para el área de TI de la empresa Quimidomsa

b. Objetivos específicos.

- Analizar todos los procesos actuales con la finalidad de revisar si existen vulnerabilidades y riesgos en alguno de estos.
- Analizar los procesos críticos de la empresa y los de mayor prioridad.
- Definir roles a cada persona que tendrán responsabilidades en el proceso de recuperación del área de TI.
- Elaborar Políticas y normas para el personal de TI en relación al cumplimento y acople del plan de recuperación.
- Capacitar y concientizar al personal sobre el plan de recuperación implementado.

4. Justificación de la investigación.

Cada día aumenta la demanda de información y la realización de los procesos y actividades de la empresa con rapidez y eficiencia, esto a su vez ha creado una dependencia de la tecnología de información en las empresas. Es por ello que se hace imprescindible para las mayorías de las empresas contar con una continuidad de negocios, donde puedan asegurar la disponibilidad de servicios en cualquier catástrofe o situación que pueda afectar esta continuidad, ya que la tendencia del mercado actual son compañías que ofrezcan servicios 24 horas o 24/7 de acuerdo a lo requerido.

Un estudio realizado por Comunicaciones World, demostró que solo un 15% de las empresas Españolas está capacitada para recuperarse de posibles desastres; Para evitar cualquier situación que pueda dejar sin funcionamiento a los sistemas informáticos, cerca de un 11% de las empresas consultadas tienen implementados algún tipo de plan de contingencia que aseguren la continuidad y la recuperación de los sistemas. Por otra parte un 34% de las empresas han matizado que tienen desarrollado un plan de contingencia de modo orientativo.

El 56% de las empresas entrevistadas tiene elaborado un plan de recuperación de la información, pero sólo el 15% lo tiene hecho de forma documentada y detallada y el 41% restante lo tiene elaborado sólo de modo orientativo. El 29% de las empresas, aunque no lo tengan elaborado, tiene previsto hacerlo y el 10% de las empresas ni siquiera tiene previsión de realizarlo. Estos datos indican que si se generara algún tipo de desastre, sólo un 15% de las empresas estaría capacitado para recuperarse de las diferentes pérdidas.

Por poner otro ejemplo, reportes del Centro Nacional para la Prevención contra Desastres de Mexico (Cenapred) indican que los huracanes Emily, Stan y Wilma en México dejaron pérdidas aproximadas de 45,000 Millones de pesos, cifra que, a decir del organismo, es seis veces mayor al promedio histórico que tiene el país por desastres de diversa índole.

Si analizamos a nuestro país, según un estudio realizado por la Asociación Dominicana de Mitigación de desastres, República Dominicana ha sido impactada desde el año 1900 al 2004 (104 años) por fenómenos de magnitud desastrosa. Los fenómenos naturales que más han atacado el país son los siguientes:

- 20 huracanes, 7 de ellos muy intensos.
- 8 inundaciones

- 4 sismos.

Refiriéndonos a estos fenómenos, han dejado un saldo aproximado de 10,606 pérdidas humanas; daños económicos estimados en 109 millones de pesos (Al año 2004 - 234 mil dólares); afectando directamente a 20 mil quinientos noventa y cinco personas.

Las cifras presentan variaciones entre este estudio y otros de la misma índole, porque en cada caso, lamentablemente, en el país no se cuenta con las herramientas necesarias para realizar un adecuado levantamiento de la información.

Un Plan de Continuidad del negocio (BCP) resulta de una metodología aplicada al interior de la empresa y se usa para crear planes logísticos sobre cómo una organización debe recuperar y restaurar sus funciones críticas de manera parcial o total después de sufrir una interrupción por un desastre o situación inesperada. También sirve para que la organización esté lista para futuros incidentes que puedan ponerla en peligro.

Por su parte, un Plan de Recuperación de desastres (DRP) es el proceso de recuperación de datos, incluyendo software y hardware críticos, para que un negocio pueda comenzar de nuevo sus operaciones en caso de una eventualidad de este tipo.

En tal sentido, es necesario implementar para el área de TI de la empresa Quimidomsa un plan recuperación de desastre (DRP). Este plan de DRP aumentará la confianza y seguridad en gran medida al personal del departamento de TI donde tendrán mayor control de la situación de emergencia, teniendo en sus manos las normas y procedimientos y además las herramientas necesarias para contrarrestar cualquier amenaza.

5. Tipo (s) de investigación.

Se desarrollo dentro de la clasificación de investigación documental y explicativa.

6. Marcos de referencia

a) Marco teórico

Plan de Continuidad del Negocio (BCP) es el resultado de la aplicación de una metodología interdisciplinaria, llamada Business Continuity Management (BCM), usada para crear y validar planes logísticos para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción o desastre. En lenguaje sencillo, BCP es el cómo una organización se prepara para futuros incidentes que puedan poner en peligro la organización y su misión básica a largo plazo.

Un DRP (Disaster Recovery Plan), consiste en preparar el área de tecnología de información para que esta pueda responder adecuadamente a un incidente que afecte la infraestructura tecnológica de la empresa. Este es el complemento crucial de un buen BCP, este define los pasos a seguir para restaurar el funcionamiento normal de un proceso. Por lo regular, está orientado a recuperar la operatividad de las aplicaciones identificadas como criticas para los procesos del negocio, en el menor tiempo posible, utilizando para ello recursos y procedimientos adecuados, con el enfoque primordial de minimizar el impacto y el costo de un desastre.

El Análisis del Impacto sobre el Negocio, (BIA) es un análisis que consiste en tener conocimientos de las datos más importantes en la empresa y de mayor prioridad, estos se clasifica en:

Críticos, vitales, sensitivos y no críticos

Las fases del BIA son: Identificación de procesos, Procesos críticos, Identificación de infraestructura, análisis de vulnerabilidades, Impacto de grupo de desastres, Impacto en costos y tiempo objetivo.

El estándar ISO 27001 contiene las normas que debe seguirse para tener un DRP adecuado ya que proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

b) Marco conceptual

BCM: Proceso de gestión integral en materia de continuidad. Analiza las amenazas relevantes y desarrolla para la organización un esquema de resistencia y de respuesta que salvaguarde de forma efectiva los intereses de las partes.

DRP (Disaster Recovery Plan): consiste en preparar el área de tecnología de información para que esta pueda responder adecuadamente a un incidente que afecte la infraestructura tecnológica de la empresa.

BIA (Business Impact analysis): Es el análisis del impacto sobre el negocio, consiste en tener conocimientos de los datos mas importantes en la empresa y de mayor prioridad. Es el que cuantifica las consecuencias de una interrupción del servicio en cada uno de los sistemas empresariales

RA (Risk Analysis): Es el estudio de las causas de las posibles amenazas, y los daños y consecuencias que estas puedan producir.

Amenazas: Es un fenómeno, proceso natural o situación provocada por el ser humano que puede poner en peligro a un grupo de personas, sus bienes y su ambiente.

Disponibilidad: es la capacidad del funcionamiento ininterrumpido de todos los servicios y recursos de TI.

Políticas: Es un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera

c) Marco espacial.

El marco espacial en el que se desarrolla este proyecto es en el municipio de Haina, provincia de San Cristóbal en la empresa Quimidomsa.

d) Marco temporal.

El periodo de ejecución de este proyecto es desarrollado en el intervalo de enero-abril 2010.

7. Métodos, procedimientos y técnicas de la investigación

b) Métodos

Para este trabajo se utilizaron los siguientes métodos:

- Métodos de Observación: Se realizaran visitas y evaluaciones generales del área de TI, y de toda la estructura organizacional empleando la observación sistemática, es decir anticipando y conociendo de antemano los aspectos en los que haremos hincapiés en este proceso de observación.

- Métodos de análisis: Utilizaremos el análisis con el fin de compilar la información y datos capturados en el proceso de observación, entrevistas y demás, con el fin de que nuestra problemática inicial quede totalmente solucionada o encaminada a hacerlo.

c) Procedimientos:

1. Realización de un análisis y evaluación de riesgos(RA) en TI
2. Realización de un análisis de impacto de negocios (BIA) en TI
3. Realización de la estrategia para el plan
4. Elaborar e implementar el plan de recuperación de desastres.
5. Definir Estrategias de capacitación
6. Definir Estrategias de pruebas
7. Definir el mantenimiento del plan de recuperación.
8. Elaboración del informe final incluyendo recomendaciones y conclusiones.
9. Entrega del informe final.

d) Técnicas de la carrera que estudia utilizadas en la investigación.

Las técnicas utilizadas son las siguientes:

- Entrevistas
- Observación de las áreas de TI.

Tabla de contenido

Apéndice II

Controles y Políticas de seguridad existentes en QUIMIDOMSA

DECLARACION DE POLITICA

"Será la responsabilidad del departamento de Tecnologías proveer la adecuada protección y confidencialidad de toda la información corporativa y de los sistemas de software propietarios, así sea centralizado, en almacenaje local, o remotamente, para asegurar la continua disponibilidad de información y programas para todos los miembros autorizados de la empresa, y asegurar la integridad de toda la información y los controles de configuración".

1. RESUMEN DE POLITICAS DE SEGURIDAD PRINCIPALES

1.1. Confidencialidad de toda la información debe ser mantenido a través de un discreto y obligatorio control de acceso.

1.2. Internet y el acceso a otros servicios externos están restringidos, solamente el personal autorizado tendrá acceso.

1.3. El acceso para la información en todas las laptop debe ser asegurado con encriptación o por otro medio, para proveer confidencialidad de la data en caso de pérdida o robo del equipo.

1.4. Solo el software autorizado y licenciado puede ser instalado, Y la instalación debe de realizarse por el personal del Departamento de Tecnologías.

1.5. El uso de software sin autorización está prohibido. En caso de que software sin autorización sea descubierto, este será removido de la estación de trabajo inmediatamente.

1.6. La información solo puede ser transferida por los propósitos determinados en la política organizacional de protección de data.

1.7. Todos los diskettes y los medios removibles de Fuentes externas deben ser revisadas por un antivirus antes de ser utilizadas en la organización.

1.8. La clave de Windows debe de consistir en una mezcla de al menos 8 caracteres, debe ser cambiada cada 40 Días y debe ser única.

1.9. Las configuraciones de las estaciones de trabajo, deben ser cambiadas solo por el Personal del Departamento de Tecnologías.

1.10. Para prevenir la perdida de disponibilidad de recursos de TI, medidas deben ser tomadas para el backup de la data, aplicaciones y la configuración de todas las estaciones de trabajo.

2. PROTECCION CONTRA VIRUS

2.1. El departamento de Tecnologías De Información tendrá disponible un software actualizado a la fecha para el escaneo de los archivos y eliminación de supuestos virus.

2.2. Los Servidores de Archivos corporativos estarán protegidos con un software de escaneo de virus.

2.3. Las estaciones de trabajo estarán protegidas con un software de escaneo de virus.

2.4. Todos los antivirus serán regularmente actualizados con la última versión de los parches por el Departamento de T.I.

2.5. Ningún disco de fuera de la organización puede ser utilizado hasta que este no haya sido escaneado.

2.6. Todos los sistemas serán instalados de una copia original, o una copia maestra limpia con la protección de escritura en su sitio. Solo copias maestras pueden ser utilizadas hasta que el antivirus sea instalado y actualizado completamente.

2.7. Todas las medias removibles que contengan software ejecutables (extensiones .EXE y .COM) serán protegidas contra escritura cuando sea posible.

2.8. Todas las demostraciones de los vendedores serán ejecutadas en sus computadoras y no las de la organización.

2.9. Shareware no puede utilizarse, como los shareware son una de las principales fuentes más comunes de infección. Si es absolutamente necesario utilizar el shareware, este debe de ser escaneado completamente con un antivirus actualizado a la fecha antes de utilizarlo.

2.10. El software comercial Nuevo debe ser escaneado antes de ser instalado porque ocasionalmente suelen tener virus.

2.11. Todos los medios removibles que vengan desde fuera de la organización traídas por los ingenieros o el personal de soporte deben de ser escaneados por el Departamento de T.I. antes de ellas ser utilizadas en la organización.

2.12. Para habilitar la recuperación de la información en caso de un brote de virus, copias de respaldo deben de tomarse por el Depto. T.I.

2.13. Administrar y aplicar con firmeza la política del antivirus de la organización y mantener siempre disponible los recursos para implementarlo.

2.14. Los usuarios deben ser informados de los procedimientos actuales y de las políticas.

2.15. Los usuarios deben ser notificados con incidentes de virus.

2.16. Los usuarios serán considerados responsables por cualquier rotura de la política de antivirus de la organización.

2.17. Las políticas y los procedimientos de los antivirus serán revisados regularmente.

2.18. En caso de una posible infección con virus, el usuario debe de informar al departamento de T.I. inmediatamente. El departamento de T.I. debe de escanear la computadora infectada y cualquier medio removible o cualquier computadora a la cual el virus pueda haberse dispersado y erradicarlo.

3. CONTROL DE ACCESO

3.1. Todos los usuarios deben de tener suficiente derecho en todos los sistemas para permitirles a ellos hacer su trabajo. El acceso de los usuarios debe de mantenerse mínimo todo el tiempo.

3.2. Las solicitudes de los usuarios para los accesos de los diferentes sistemas, deben de hacerse a través del sistema de soporte del Depto. de T.I.

3.3. Nadie debe tener acceso ilimitado en ningún sistema. El Depto. de T.I. controlara las contraseñas de los servidores y de la red y las contraseñas de los sistemas serán asignados por el administrador de sistemas en el departamento del usuario final. El administrador de sistemas será responsable por el mantenimiento de la integridad de la información del departamento del usuario final y por la determinación de los accesos de los usuarios finales.

3.4. El acceso para la red/servidores y sistemas deben de ser con el usuario de administrador de sistemas y cuando sea posible con un nombre de usuario único y contraseña única.

3.5. Los nombre de usuario y claves no deben de ser compartidos por usuarios.

3.6. Los nombre de usuario y claves no deben de ser escritos.

3.7. Los nombre de usuario consistirán de el primer nombre seguido de la primera letra del apellido.

3.8. Todos los usuarios tendrán una clave alfanumérica de cómo mínimo 8 caracteres.

3.9. Las contraseñas de Windows expiraran a los 40 Días y deben de ser única.

3.10. La detección de intrusos será implementada donde sea posible. La cuenta del usuario será bloqueada después de 3 intentos erróneos.

3.11. El departamento de Tecnologías será informado con anticipación de todos los empleados que dejen de laborar con la organización. El Depto. de Tecnologías deshabilitara al usuario de todos los sistemas.

3.12. La contraseña del administrador de la Red, y los servidores debe de ser resguardada en un lugar seguro en caso de emergencias o desastres.

3.13. Auditoria debe de ser implementada en todos los sistemas para registrar los intentos de entrada fallidos, intentos correctos y cambios hechos a todos los sistemas.

3.14. El Personal del Dpto. de T.I. no se logueara como root en ningún sistema UNIX, LINUX, pero podrá utilizar el comando su para obtener privilegios administrativos.

3.15. La contraseña por defecto en los sistemas como Oracle y SQLServer debe de ser cambiada después de la instalación.

3.16. En los sistemas UNIX y LINUX, el privilegio para rlogin, ftp, telnet, ssh será restringido para el personal del Depto. de T.I.

3.17. Solo si es necesario se le dará acceso a los usuarios al Shell Prompt de UNIX o LINUX.

3.18. Archivos de sistemas deben de tener la máxima seguridad implementada que sea posible. Donde sea posible los usuarios solo deben tener privilegios de lectura y escaneo de directorios, los archivos serán señalados como solo lectura para prevenir que se borren por accidente.

4. SEGURIDAD EN LA RED DE AREA LOCAL (LAN)

- HUB & Switches

4.1. Los equipos de la LAN, hubs, bridges, repeaters, routers, switches estarán en un gabinete seguro. El cuarto donde estarán el gabinete estará cerrado todo el tiempo. El acceso al cuarto del gabinete/rack será restringido solo para la entrada del Dpto. de T.I. Cualquier otra persona o contratista que requiera acceso a cuarto del gabinete/rack debe de notificar al Dpto. de T.I. para que la supervisión necesaria sea arreglada.

- Estaciones de Trabajo

4.2. Los usuarios deben de cerrar o bloquear su sección cuando dejen sus estaciones de trabajo en cualquier momento. Alternativamente las estaciones de trabajo de Windows deben de ser bloqueadas.

4.3. Todas las estaciones de trabajo que no se estén utilizando fuera del horario de trabajo, deben de ser apagadas.

- Alambrado

4.4. Todo el alambrado debe de estar Documentado

4.5. Todos los puntos de red que no estén en uso, deben de ser desactivados.

4.6. Los usuarios no deben de poner o almacenar ningún artículo sobre el cableado de la red.

4.7. Cableado redundante debe de ser usado donde sea necesario.

- Software de Monitoreo

4.8. El uso de software analizador de LAN y analizador de paquetes está restringido y solo el Depto. de T.I. puede utilizarlos.

4.9. Los analizadores de Paquetes y de LAN deben de ser guardados con seguridad cuando no se estén utilizando.

4.10. Sistemas de detección de intrusos serán implementados para detectar acceso no autorizado a la red.

- Servidores

4.11. Todos los servidores se almacenaran en un lugar seguro y bajo llave.

4.12. El acceso a las consolas de los servidores y a los Disks/tapes deben de ser restringidos para el uso exclusivo del personal de Tecnologías.

- Seguridad Eléctrica

4.13. Todos los servidores deben de ser instalados con un UPS que incluso acondicione el suministro de energía.

4.14. Todos los Hubs, bridges, repeates, routers, switches y cualquier otro equipo crítico de la red, debe de suministrársele energía acondicionada de un UPS.

4.15. En caso de que haya una falla en el suministro principal de energía eléctrica, el UPS debe de tener suficiente energía para mantener la red y servidores operativos hasta que el generador encienda.

4.16. Todos los UPS deben de probarse periódicamente.

• Administración de Inventario

4.17. El departamento de T.I. debe mantener un inventario completo de todos los computadores y el software en uso en toda la compañía.

4.18. Auditoria anual serán llevadas a cabo para determinar las copias de software no autorizados y los cambios no autorizados en el hardware de los equipos.

• Infraestructura Física

4.19. La inclusión de equipos personales dentro de la red de la empresa o dentro del dominio de la empresa, deben de ser aprobados por el Gerente del Dpto. de Tecnologías.

4.20. La reparación y/o mantenimiento de equipos personales por el personal del Dpto. de Tecnologías, debe de ser autorizado por el Gerente del Departamento.

4.21. La compra y/o desecho de equipos del Dpto. de Tecnologías, deben de ser aprobados por el Gerente del Depto. De Tecnologías.

5. SEGURIDAD ESPECÍFICA DE SERVIDORES

5.1. Esta sección aplica para los servidores Windows, UNIX, LINUX y NOVELL.

5.2. El sistema operativo debe de estar actualizado a la fecha y parchado regularmente.

5.3. Los servidores deben de ser escaneados diariamente por un antivirus.

5.4. Los servidores deben de estar encerrados en un cuarto seguro.

5.5. Donde sea apropiado la consola del servidor puede ser activada.

5.6. Las contraseñas de administración remota debe ser diferente a las contraseñas del admin/ administrator/root.

5.7. Los usuarios que posean privilegios Admin/Administrator/root deben ser limitados a miembros entrenados del Depto. de T.I.

5.8. El uso de las cuentas Admin/administrator/root deben de utilizarse lo menos posible.

5.9. La asignación de seguridad equivalente que le de a un usuarios el mismo privilegio que otro usuario debe de ser evitado donde sea posible.

5.10. El acceso a la data y las aplicaciones deben de ser limitado por controles de accesos.

5.11. Detección de Intruso y bloqueo deben ser habilitados.

5.12. Las facilidades de auditoría deben de ser habilitadas.

5.13. Los usuarios deben de bloquear o cerrar la sección cuando se alejen de su estación de trabajo.

5.14. Todas las estaciones de trabajo que no están en uso fuera del horario de trabajo, deben de ser apagadas.

5.15. Todas las cuentas deben de tener asignada una contraseña de por lo menos 8 caracteres.

5.16. El número de conexiones concurrentes debe de ser limitada a 1.

5.17. En ciertas áreas los usuarios deben de ser restringidos a loguearse en horas de trabajo solamente.

6. SEGURIDAD ESPECIFICA DE UNIX & LINUX

6.1. Acceso directo del root debe ser limitado para el uso solo de consola.

6.2. El personal de Dpto. de T.I. que requiera acceso con el root debe de utilizar el comando "su".

6.3. El uso de una cuenta root debe de ser utilizada lo menos posible.

6.4. Todas las cuentas de UNIX y LINUX deben ser protegidas por contraseñas.

6.5. SSH será restringido solo para el personal autorizado.

6.6. El acceso a la data y a las aplicaciones será limitado por el ACL.

6.7. Los usuarios no tendrán acceso al nivel su($).

6.8. Todas las cuentas tienen que tener una contraseña asignada de por lo menos 8 caracteres.

6.9. Los usuarios deben de cambiar su clave cada 40 Días.

7. WIDE AREA NETWORK SECURITY

7.1. Las Redes de área local inalámbricas deben de utilizar los métodos más seguros de encriptación y autenticación disponibles.

7.2. Los usuarios no instalaran sus propios equipos inalámbricos bajo ninguna circunstancia.

7.3. Dial-in módems no deben de utilizarse. Un túnel VPN es la opción predeterminada.

7.4. Todos los Bridges, Routers and Gateways deben de mantenerse bajo llave en un área segura.

7.5. Los protocolos innecesarios, se deben de eliminar de todos los routers.

7.6. El método preferido para conectarse desde fuera de la empresa es el VPN, utilizando PPTP o L2/IPSEC.

7.7. Todas las conexiones hechas desde fuera de la red, deben ser registradas.

8. TCP/IP & SEGURIDAD DE INTERNET

8.1. Las conexiones permanentes al internet deben hacerse por medio de un Firewall y/o proxy para regular el tráfico de la red.

8.2. Las conexiones permanentes a otras redes externas, deben de ser a través del Firewall para regular y asegurar el tráfico de la red.

8.3. El equipo de red debe ser configurado para cerrar las secciones inválidas.

8.4. Cuando los usuarios se conecten por VPN, estas conexiones deben ser situadas en el DMZ o en una red no segura fuera del firewall.

8.5. Las estaciones de trabajo que accedan al internet, deben de hacerlo a través del Proxy de la organización y a través del los filtros de contenido.

8.6. Todos los emails entrantes deben de ser escaneados por el filtro de contenido, el antivirus y el antispam de la organización.

9. SEGURIDAD EN EL SISTEMA DE VOZ

9.1. El puerto de mantenimiento de la PBX será protegido por una contraseña segura.

9.2. La contraseña de administrador de la PBX se deberá cambiar cada 40 días.

9.3. Se llevaran registros de llamadas para todas las llamadas salientes.

9.4. Se llevaran registros por usuarios de llamadas para las llamadas de larga distancia nacional.

9.5. Se llevaran registros por usuarios de llamadas para las llamadas a celulares.

9.6. Se llevaran registros por usuarios de llamadas para las llamadas de larga distancia internacional.

9.7. Los buzones de voz deben de tener una contraseña con un mínimo de 4 caracteres.

9.8. La contraseña nunca debe ser la misma que el número de la estación.

9.9. El buzón de correo cerrara la sección luego de tres intentos fallidos con la contraseña.

9.10. Las cuentas telefónicas deben de ser revisadas periódicamente para evitar consumos injustificados.

Apéndice III

Cuestionario

Análisis de

Impacto del

Negocio

Nombre: _____

Cargo: _____

Departamento: _____

Fecha: _____

Favor responder cada pregunta de acuerdo a las informaciones de la empresa.

1. **Los procesos de negocio** ¿Cuáles son los procesos que tiene a cargo la unidad de negocios? Cuanto tiempo usted cree que debe durar para recuperarse cada proceso señalado?

2. **Atrasos**- Para cada proceso anterior, ¿cuánto tiempo tomará (en horas) a manejar los procesos para cada día del tiempo de inactividad?

3. **Informes Regulatorios**-¿Se tiene algún informe reglamentario requerido? Escriba el nombre del informe, el receptor, la frecuencia, y el tipo de penalidad (Cantidad, si los hubiera).

4. **Complejidad de la restauración:** defina la complejidad para la restauración(señale)

Fácil recuperables Algo recuperable Difícil de recuperar Muy difícil recuperarse.

5. **Interrupción de la tolerancia Bajo el peor de los casos**, ¿cuánto tiempo (horas o días) su unidad de negocio podría ser completamente paralizadas antes de que hubiera una significativo impacto en la muestra en su conjunto, las unidades de negocio, socios comerciales, regulador cumplimiento?

6. **Perfil Impacto Mensual** - Por cada mes, definir la gravedad de la interrupción donde 0 = Sin impacto, 4 = Impacto severo.

Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sept	Oct	Nov	Dic

¿Qué tipo de impacto para cada uno de los de arriba: financieros, operativos y otros?

---

7. **Impacto que los factores operacionales**-Para los siguientes impactos operativos, definir el la gravedad del impacto, donde 0 = sin impacto, 4 = severo impacto.

Operación	Valor
Flujo de Caja	
Ventaja Competitiva	
Confianza del cliente	
Reportes financieros	
Imagen del negocio	
Moral del Empleado	
Servicio al Cliente	
Comisiones	
Proveedores	
Entidades Regulatorias	
Otros	

---

8. **Impactos financiero acumulativos estimado por día**-Estimar los recursos financieros impacto en su unidad de negocio en el peor de los emitidos por días o semanas como la siguiente manera:

Día 1	Día 2	Día 3	Día 4	Día 5	Día 6	Día 7	Día 14	Día 21	Día 28

9. **La confianza en las comunicaciones**-Identificar la dependencia de la pérdida de las comunicaciones, tales como teléfonos, correo electrónico, etc,
donde 0 = sin impacto, 4 = severo impacto.

10. **Otras cuestiones y preocupaciones-**Identificar cualquier problema o preocupación relacionada con la recuperación de su unidad de negocio que no se han discutido.

Apéndice IV

Cotizaciones de Hardware para estrategias

PROPUESTA ECONOMICA

CLIENTE	COMENTARIOS
Quimidomsa República Dominicana Atención: Ryan Corominas	No esta Incluido el Servicio de Instalacion.

Propuesta	Fecha	Teléfono	Fax	Consultor
EVA4400-01				

CANT	DESCRIPCIÓN	PRECIO UND	US$ TOTAL
1	**HP EVA4400 146GB HDD Field Starter Kit** **Unidad de almacenamiento:** 146GB, 15K rpm, Fibre Channel. **Nº de unidades:** 8 incluidas **Controlador de almacenamiento:** 2 HSV300 **Enclosure Type(Tipo de receptáculo):** Admiten hasta 8 carcasas M6412 **Sistemas operativos compatibles:** HP-UX; HP OpenVMS; Linux; Sun Solaris; Windows® Server 2003 Standard Edition (32 bits/x64); Windows® Server 2003 Enterprise Edition (32 bits/x64; Windows® Server 2008 Standard Edition (32 bits/x64); Windows® Server 2008 Enterprise Edition (32 bits/x64); Windows® Server 2008 Server Core; VMware; Novell NetWare; IBM AIX; Apple Mac OS X **EVA4400 Startertr Kit JW Supp:** 1 Unidad **HP 24A High Voltage US/JP Modular PDU:** 2 Unidades **HP PCI-X 2.0 1Port 4Gb Fibre Channel HBA:** 4 Unidades **HP 2m Multi-mode OM3 LC/LC FC Cable:** 4 Unidades **Warranty: HP 3y Support Plus 24 SVC**	46,219.27	46,219.27

Sub-total	46,219.27
Otros Gastos	-
ITBIS	7,395.08
US$ TOTAL	**53,614.35**

CONDICIONES:

- Forma de Pago: 50% con la orden, 50% contra entrega.
- Tiempo de Entrega: 25 dias.
- Precios Válidos por: 7 días

Segunda cotización

DELL

QUOTATION / COTIZACIÓN

QUOTE/Cotización #: **123**

Customer #/Cliente #: **3652356**

Date of Quote/Fecha de Cotización:

Customer/Cliente: **Quimidomsa**

TOTAL QUOTE AMOUNT / Total de la Cotización:	$2,285.51		
Subtotal / Subtotal:	$1,932.51		
Tax/Impuesto:	$0.00		
Shipping and Handling / Envío y Manejo:	$353.00		
		Total Number of System Groups / Total de grupos en la cotización:	1

All amounts shown are in US Dollars / Los precios son en dólares de los Estados Unidos

GROUP / GRUPO: 1	QUANTITY / CANTIDAD: 1	SYSTEM PRICE / PRECIO DEL SISTEMA: $1,932.51	GROUP TOTAL / TOTAL DEL GRUPO: $1,932.51
Base Unit \ Unidad base:		Quad Core Xeon X3363 Processor2x6M Cache, 2.83GHz, 1333MHz FSB for PowerEdge R300 (223-6133)	
Memory \ Memoria:		24GB DDR2, 667MHz, 6x4GB Dual Ranked DIMMs (311-8354)	
Video Memory \ Memoria Video:		Riser with 2 Slots: 2 PCI Exprx8 slots (320-6326)	
Hard Drive \ Disco Duro:		750GB 7.2k RPM Serial ATA 3Gbps 3.5-in Cabled Hard Drive (341-6087)	
Operating System \ Sistema Operativo:		No Operating System (420-6320)	
NIC \ NIC/Tarjeta de red:		On-Board Dual Gigabit Network Adapter (430-2008)	
CD-ROM or DVD-ROM \ Bahia de CD-ROM o DVD-ROM:		8X DVD-ROM Drive, Internal SATA (313-6116)	
Sound Card \ Tarjeta de Sonido:		Bezel (313-6114)	
Speakers \ Parlantes:		Chassis with Cabled Hard Driveand Non-Redundant Power Supplyfor PowerEdge R300 (330-0309)	
Documentation Diskette \ Diskette De Documentación:		Dell Management Console (330-5280)	
Documentation Diskette \ Diskette De Documentación:		Electronic Documentation and OpenManage DVD Kit (330-0312)	
Additional Storage Products \ Productos Adicionales De Almacenaje:		750GB 7.2k RPM Serial ATA 3Gbps 3.5-in Cabled Hard Drive (341-6087)	
Feature \ Caracteristica:		Add-in SAS6IR RAID Controller (SATA/SAS Controller) which supports 2 Hard Drives - RAID 1 (341-6341)	
Feature \ Caracteristica:		Sliding Rapid/Versa Rails and Cable Management Arm,Universal (341-3090)	
Service \ Servicio:		Dell Hardware Limited Warranty Plus On Site Service Extended YR (912-2788)	
Service \ Servicio:		Basic: Business Hours (5X10) Next Business Day On Site Hardware Limited Warranty Repair Init YR (914-1800)	
Service \ Servicio:		Dell Hardware Limited Warranty Plus On Site Service Inital YR (912-2947)	
Service \ Servicio:		DECLINED CRITICAL BUSINESS SERVER OR STORAGE SOFTWARE SUPPORT PACKAGE-CALL YOUR DELL SALES REP IF UPGRADE NEEDED (912-2967)	
Service \ Servicio:		Basic: Business Hours (5X10) Next Business Day On Site Hardware Limited Warranty Repair 2YR Ext (914-2342)	