

UNIVERSIDAD NACIONAL AUTÓNOMA DE HONDURAS
POSTGRADO DE LA FACULTAD DE CIENCIAS ECONÓMICAS

POSFACE

DIRECCIÓN DEL SISTEMA DE ESTUDIOS DE POSTGRADO

MAESTRÍA EN GESTIÓN INFORMÁTICA



TESIS

**IMPLEMENTACIÓN Y EVALUACIÓN DE UN PLAN DE
CONTINUIDAD DEL NEGOCIO DE LOS SERVICIOS DE
TECNOLOGÍA, EN DROGUERÍA Y LABORATORIO HENIE
FARMA S. DE R.L., EN TEGUCIGALPA.**

SUSTENTADA POR

IBIS JAVIER ZAVALA RODRÍGUEZ

**PREVIO A OPTAR AL TÍTULO DE
MÁSTER EN GESTIÓN INFORMÁTICA**

TEGUCIGALPA, HONDURAS MAYO DEL 2022

AUTORIDADES UNIVERSITARIAS

DR. FRANCISCO JOSE HERRERA ALVARADO
RECTOR

MAE. BELINDA FLORES DE MENDOZA
VICERRECTORA ACADÉMICA

DRA. JESSICA PATRICIA SÁNCHEZ MEDINA
SECRETARIA GENERAL

Dr. RAÚL ARMANDO EUCEDA
DIRECTOR DE POSGRADOS

MAE. OSCAR ARQUÍMEDES ZELAYA
DECANO DE LA FACULTAD
DE CIENCIAS ECONÓMICAS

DR. LUIS ARMANDO DUARTE HERNÁNDEZ
COORDINADOR GENERAL DEL POSGRADO DE LA
FACULTAD DE CIENCIAS ECONÓMICAS
(POSFACE)

Dedicatoria

En nuestra estadía por este mundo nos encontramos con una infinidad de retos, y para mí la educación de Postgrado era uno de ellos. Después de experimentar este tiempo de conocimiento, he llegado a la conclusión que más allá de ser un reto, es una plataforma sólida no solo para el entendimiento del área en el que me he visto inmerso, sino para todo lo que involucra el crecimiento personal y profesional.

Dedico este logro a Dios y toda mi familia, por su apoyo incondicional durante todo el proceso, a todas aquellas personas que influyeron en el desarrollo de este trabajo mediante sus aportes; anhelando que este trabajo influya de manera positiva a la empresa representada o cualquiera que lo adopte, gracias.

Agradecimiento

Agradezco infinitamente a Dios, ya que me dio la vida y la fortaleza para culminarlo con éxito; a mis padres Francisco Javier Zavala y Virginia Isabel Rodríguez por todas sus muestras de cariño y apoyo en todos estos años, gracias a ustedes me he formado como un excelente ser humano y he logrado este gran objetivo.

A mi abuelo René Alfredo Zavala (QDDG) quien dejó una huella imborrable en mi vida, y me enseñó que en la vida hay que luchar por lo que se quiere y nunca darse por vencido; aunque él no esté físicamente conmigo, sé que su espíritu vivirá por siempre en mi corazón.

A mi amada esposa Emma Isaura Rodríguez que se ha convertido en ese motor que me impulsó durante todo este ciclo educativo, que con su apoyo incondicional se ha convertido en amiga y compañera inseparable, fuente de humildad, sabiduría, calma y consejo; tu ayuda ha sido indispensable e incluso has estado conmigo en la adversidad, este proyecto no ha sido fácil pero siempre has estado ahí motivándome a no desfallecer; te lo agradezco muchísimo amor.

A mis hijos Liam Isaac y Emmy Sofía, su cariño y amor son los motivos de mi felicidad, de mi sacrificio, de mi esfuerzo por darles lo mejor, aún a sus cortas edades me han dado muchas lecciones de vida; les agradezco hijos por ayudarme a encontrar ese lado dulce de la vida; son mi mayor motivación para concluir con éxito este proyecto, gracias, hijos míos.

Resumen

El presente trabajo de investigación trata sobre la importancia de disponer de un plan de continuidad de negocios en Droguería y Laboratorio Henie Farma S. de R.L., siendo el principal objetivo identificar los servicios y equipos tecnológicos críticos, sus riesgos y amenazas a los que se encuentran expuestos, de esta manera adaptar a la realidad de la empresa una propuesta ideal de plan de continuidad de negocios.

Es fundamental tener un correcto manejo de riesgos y una visión clara de las actividades a realizar para recuperar o restaurar las operaciones tecnológicas ante posibles amenazas materializadas, presencia de desastres naturales como terremotos, sismos, incendios, inundaciones o delincuencia que pueden afectar notoriamente el desempeño ideal de la institución. Henie Farma es una empresa del sector farmacéutico dedicada a la fabricación y comercialización de productos fármacos de calidad, es una empresa orientada al cuidado de la salud y a mejorar la calidad de vida de sus clientes, cumpliendo con las buenas prácticas de manufactura para producir productos que poseen una calidad que se percibe desde el primer momento de uso logrando así una “Calidad que se siente”. se enfocan en darles valor a los socios, empleados y la comunidad que sirven.

El contenido de este trabajo refleja la estrategia y modelo de un plan de continuidad de negocio, diseñado a la medida de la empresa Henie Farma y siguiendo estándares internacionales respecto a temas de continuidad de servicios tecnológicos, la aplicabilidad de la propuesta brinda un panorama amplio de los resultados positivos que se pueden obtener al implementar un plan bien estructurado.

Abstract

This research paper deals with the importance of having a Business Continuity plan in Droguería y Laboratorio Henie Farma S. de R.L., the main objective being to identify critical technological services and equipment, their risks, and threats to which they are exposed, in this way adapt to the reality of the company an ideal proposal for a business continuity plan.

It is essential to have a correct risk management and a clear vision of the activities to recover or restore technological operations in the face of possible materialized threats, presence of natural disasters such as earthquakes, earthquakes, fires, floods, or crime that can notoriously affect the ideal performance of the institution. Henie Farma is a company in the pharmaceutical sector dedicated to the manufacture and marketing of quality pharmaceutical products, it is a company oriented to health care and to improve the quality of life of its customers, complying with good manufacturing practices to produce products that have a quality that is perceived from the first moment of use thus achieving a "Quality that is felt". they focus on giving value to the partners, employees, and community they serve.

The content of this work reflects the strategy and model of a business continuity plan, designed to suit the company Henie Farma and following international standards regarding issues of continuity of technological services, the applicability of the proposal provides a broad overview of the positive results that can be obtained by implementing a well-structured plan.

Índice general

Dedicatoria.....	III
Agradecimiento.....	IV
Resumen.....	V
Abstract.....	VI
Índice general.....	VII
Índice de tablas y figuras.....	XI
Listado de símbolos y Abreviaturas.....	XIII
Introducción.....	1
Capítulo I: Planteamiento del problema.....	3
1.1 Antecedentes de la Investigación.....	3
1.2 El problema de investigación.....	8
1.3. Preguntas de Investigación.....	9
1.4 Objetivos de la Investigación.....	10
1.4.1 Objetivo General.....	10
1.4.2 Objetivos Específicos.....	10
1.5 Justificación del Estudio.....	10
1.6 Delimitación del Problema.....	13
1.7 Viabilidad del Estudio.....	14
1.7.1 Viabilidad Técnica-funcional.....	14
1.7.1.1 Operativa.....	14
1.7.1.2 Recursos Financieros.....	14
1.7.1.3 Recursos Humanos.....	15
1.7.1.4 Acceso a fuentes.....	15
Capítulo II. Fundamentos Teóricos de la Investigación.....	16
2.1 Marco Referencial.....	16
2.1.1 Requerimientos: Análisis de Impacto del Negocio.....	16
2.1.2 Objetivos y Alcance del Análisis de Impacto del Negocio.....	17
2.1.3 Identificar Procesos y Funciones.....	17
2.1.4 Evaluaciones del BIA.....	18

2.1.4.1	Procesos y funciones, Henie Farma	18
2.1.4.2	Contexto de la Evaluación del Impacto Financiero y Operacional	21
2.1.4.2.1	Contexto: Evaluación del Impacto Financiero.....	21
2.1.4.2.2	Contexto: Evaluación del impacto operacional	22
2.1.4.3	Identificar Procesos Críticos del Negocio	23
2.2	Marco Teórico.....	24
2.2.1	¿Qué es un Plan de Recuperación de Desastres?.....	24
2.2.2	¿Para qué se necesita un plan de continuidad del negocio?.....	25
2.2.3	¿Plan de Contingencias o Plan de Continuidad?	26
2.2.4	En materia: Plan de Continuidad del Negocio (Bussines Continuity Plan por sus siglas en inglés BCP).....	27
2.2.5	Análisis de Impacto del Negocio (Business Impact Analysis por sus siglas en inglés BIA)	28
2.2.6	Evaluación de riesgos.....	29
2.2.7	Plan de continuidad del negocio de acuerdo con el estándar británico BS25999.....	30
2.2.8	¿Se está evaluando la Resiliencia de la infraestructura tecnológica en la empresa?	31
2.3	Marco Conceptual.....	32
2.3.1	Máximo Tolerable de Caídas.....	32
2.3.2	Tiempo Disponible de Recuperación.....	32
2.3.3	Punto Objetivo de Recuperación	33
2.4	Marco Histórico Contextual	39
2.4.1	América Latina y el Caribe.....	39
2.4.1.1	Amenazas naturales.....	40
2.4.1.2	Amenazas causadas por el hombre	43
2.4.1.3	Amenazas causadas por fallo de la tecnología por razones no atribuibles a la.....	44
	naturaleza o al hombre	44
2.4.2	Contexto Nacional.....	45
2.5	Marco Legal.....	45
2.5.1	Circular CNBS No.119/2005.....	45
2.5.2	Proyecto De Reformas A La Norma De Gestión De Riesgo Operativo.....	47
2.6	Marco Normativo.....	49
2.6.1	ISO 27001.....	49
2.6.2	ISO 22301.....	50

2.6.3 COBIT	50
2.6.4 ITIL	51
2.6.5 NIST SP 800-34.....	51
2.7 Marco Institucional	52
Capítulo III. Metodología	55
3.1 Enfoque de investigación	55
3.2 Tipo de Investigación.....	56
3.3 Diseño de Investigación	56
3.4 Población y Muestra.....	57
3.4.1 Tipo de muestreo.....	58
3.4.2 Cálculo de la muestra.....	58
3.5 Instrumentos y Técnicas de Recolección de Información	59
3.5.1 Técnicas de Recolección de Información	59
3.5.2 Instrumentos de Recolección de Información	60
3.5.2.1 Evaluación Preliminar del Plan de Continuidad del Negocio	61
3.5.2.2 Plantilla para registrar la Conformación de Equipos	61
3.5.2.3 Lista de Chequeo de Notificaciones.....	61
3.5.2.4 Lista de Chequeo de Respuesta	61
3.5.2.5 Evaluación de Análisis de Impacto del Negocio (BIA).....	61
3.5.2.6 Plantilla de Activación, Recuperación y Restauración del Plan	62
3.5.2.7 Plantilla de Pruebas de los Simulacros.....	62
3.5.2.8 Plantilla de Experiencia del usuario posterior a los simulacros	62
3.5.3 Proceso de Validación de Instrumentos y Técnicas	63
3.6 Plan de Análisis	63
3.6.1 Métodos y modelos de análisis de datos.	64
3.6.2 Programas por utilizar para análisis de datos.	65
3.7. Operacionalización de Variables.....	66
3.8. Hipótesis.....	67
3.8.1 Hipótesis de trabajo o de investigación.....	68
3.8.2 Hipótesis nula.	68
Capítulo IV. Resultados del Estudio y Análisis de Resultados.....	69
4.1 Pretest.....	69

4.2 Postest.....	90
4.3 Comparativo: Simulacro #1 (Pre-Test) VRS Simulacro #2 (Post-Test)	110
4.4 Análisis de resultados a la luz de la hipótesis	113
Capítulo V. Conclusiones.....	116
Capítulo VI. Aplicabilidad	118
6.1 Nombre de la Propuesta	118
6.2 Introducción.....	118
6.3 Descripción del Plan de Acción	118
6.3.1 Objetivo General	120
6.3.2 Propósito	120
6.3.3 Productos	120
6.3.4 Actividades	120
6.3.5 Indicadores.....	121
6.4 Presupuesto.....	121
6.5 Evaluación Financiera.....	122
6.6 Cronograma de Ejecución	122
6.7 Desarrollo	122
6.7.1 Identificar Sistemas y Aplicaciones Críticas de TI por Proceso del Negocio	122
6.7.2 Análisis del daño que causa la interrupción de un proceso.....	125
6.7.3 Etapas del desarrollo el plan de continuidad del negocio (Aplicabilidad)	125
6.7.3.1 Fase Inicial. (Evaluación).....	125
6.7.3.2 Fase 1. Análisis de la empresa (Evaluación).....	126
6.7.3.3 Análisis de los riesgos (Análisis y Planificación).....	126
6.7.3.4 Fase 2. Establecer Estrategia de Continuidad (Planificación).....	126
6.7.3.5 Fase 3. Respuestas (Viabilidad).....	127
6.7.3.6 Fase 4. Seguimiento (Ejecución y Recuperación)	127
6.7.3.7 Fase 5. Socialización (Ejecución y Recuperación).....	127
6.8 Definición y Ejecución del Plan de Pruebas (Simulacros)	128
Referencias.....	129

Índice de tablas y figuras

Tablas

Tabla 1. Detalle de procesos críticos y su impacto económico.	12
Tabla 2. Procesos y funciones en Henie Farma.	18
Tabla 3. Población: usuarios que utilizan servicios de TI por país.....	57
Tabla 4. Población: usuarios que utilizan servicios de TI en Oficina Tegucigalpa.....	59
Tabla 5. Operacionalización de la variable independiente.....	66
Tabla 6. Operacionalización de la Variable Dependiente	67
Tabla 7. BIA: valoración del impacto Financiero.....	77
Tabla 8. BIA: valoración del impacto reputacional.	77
Tabla 9. BIA: valoración del impacto operacional.	78
Tabla 10. Plantilla de Activación (Sistemas y Servicios): Simulacro.....	80
Tabla 11. Plantilla de Activación (Equipos): Simulacro	82
Tabla 12. Plantilla de Recuperación (Servicios y Sistemas): Simulacro	83
Tabla 13. Plantilla de Recuperación (Equipos): Simulacro.....	85
Tabla 14. Plantilla plan de restauración (servicios y sistemas): Simulacro.	86
Tabla 15. Plantilla de Restauración (Equipos): Simulacro.....	88
Tabla 16. Experiencia de usuario.	89
Tabla 17. BIA: Valoración del Impacto Financiero	97
Tabla 18. BIA: Valoración del Impacto reputacional.....	97
Tabla 19. BIA: Valoración del Impacto operacional	98
Tabla 20. Plantilla de Activación (Sistemas y Servicios): Simulacro.....	100
Tabla 21. Plantilla de Activación (Equipos): Simulacro	102
Tabla 22. Plantilla de Recuperación (Servicios y Sistemas): Simulacro	103
Tabla 23. Plantilla de Recuperación (Equipos): Simulacro.....	105
Tabla 24. Plantilla de Restauración (Servicios y Sistemas): Simulacro	106
Tabla 25. Plantilla de Restauración (Equipos): Simulacro.....	108
Tabla 26. Experiencia de usuario.	109
Tabla 27. Comparativo: Simulacro #1 (Pre-Test) VRS Simulacro #2 (Post-Test).....	110
Tabla 28. Valores porcentuales de la eficacia de la ejecución del plan de continuidad de negocio, para Henie Farma, año 2021.....	114
Tabla 29. Sistemas, aplicaciones y servicios críticos de TI.....	123
Tabla 30. Equipos para los servicios críticos de TI.....	124

Figuras

Figura 1. Elementos del Plan de Recuperación de Desastres	25
Figura 2. Estructura Plan de Continuidad del Negocio.	27
Figura 3. Ciclos del BIA.....	28
Figura 4. Gestión del Riesgo.....	29
Figura 5. Proceso Metodológico según BS-25999.....	30
Figura 6. Objetivo general de Recuperación	34
Figura 7. Documentación de los planes de continuidad	69
Figura 8. Proveedores externos que apoyen en la continuidad del negocio.....	69
Figura 9. Documentación del plan de manejo de crisis.....	70
Figura 10. Existencia de Sitio Alterno.....	70
Figura 11. Calendarización de un plan de pruebas.	71
Figura 12. Notificación de incidentes.	72
Figura 13. Detalle de Notificaciones.	72
Figura 14. Escalamiento gerencial.....	73
Figura 15. Data Center Alterno.	73
Figura 16. Coordinador de respuesta a emergencias.....	74
Figura 17. Comité de respuesta a emergencias.....	74
Figura 18. Sistemas de alarma.....	75
Figura 19. Procedimiento de evacuación para personal clave.	75
Figura 20. Periodicidad del plan de respuesta a emergencias.....	76
Figura 21. Documentación de los planes de continuidad	90
Figura 22. Proveedores externos que apoyen en la continuidad del negocio.....	90
Figura 23. Documentación del plan de manejo de crisis.....	91
Figura 24. Existencia de Sitio Alterno.....	91
Figura 25. Calendarización de un plan de pruebas.	92
Figura 26. Notificación de incidentes.	93
Figura 27. Detalle de Notificaciones.	93
Figura 28. Escalamiento gerencial.....	94
Figura 29. Data Center Alterno.	94
Figura 30. Coordinador de respuesta a emergencias.....	95
Figura 31. Comité de respuesta a emergencias.....	95
Figura 32. Sistemas de alarma.....	95
Figura 33. Procedimiento de evacuación para personal clave.	96
Figura 34. Periodicidad del plan de respuesta a emergencias.....	96
Figura 35. Resultado “t de student” con minitab v20.3 para variable X.....	115

Listado de símbolos y Abreviaturas

USD\$: dólares americanos

PIB: Producto Interno Bruto

TI: Tecnología de la Información

S. de R. L: Sociedad de Responsabilidad Limitado

BPF: Buenas Prácticas de Fabricación.

IBM: International Business Machines Corporation

SELA: Sistema Económico Latinoamericano y del Caribe

BCP: Business continuity planning

ISO: International Organization for Standardization

IEC: Comisión Electrotécnica Internacional

ITIL: Information Technology Infrastructure Library

UNAH: Universidad Nacional Autónoma de Honduras

BIA: Business Impact Analysis

SAR: Servicio de Administración de Rentas

ERP: Enterprise Resource Planning

DRP: plan de recuperación ante desastres

RTO: Tiempo objetivo de recuperación

RPO: Recovery Point Objective

MTD: Máximo de caídas Tolerables

NFPA: Asociación Nacional de Protección contra el Fuego

OEA: Organización de Estados americanos

CNBS: Comisión Nacional de Banca y Seguros

Introducción

La constante evolución de las tecnologías de la información aplicables a la industria farmacéutica, plantean un marco de disponibilidad, integridad y seguridad de la información para la operatividad de las instituciones, los cuales deberán ser respaldados por una gestión, unas políticas y unos procedimientos adecuados, que resalten el papel de las personas como el primer eslabón de una compleja cadena de responsabilidades y que esté orientado a preservar los pilares fundamentales de la seguridad y privacidad de la información.

La implementación de un proceso de preservación de la información ante situaciones disruptivas permite minimizar el impacto y recuperación por pérdida de activos de información de la organización, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación. Dentro de la gestión de la disponibilidad y seguridad de la información en las empresas, es importante contar con un plan alternativo que asegure la continuidad de las actividades u operaciones del Negocio en caso de que ocurran incidentes graves, es importante mencionar que tradicionalmente, los planes de continuidad, denominados planes de contingencia en sus orígenes están asociados a grandes compañías que necesitan reaccionar de forma inmediata ante cualquier evento que interrumpa sus servicios, la realidad es que cualquier compañía puede sufrir un incidente que afecte a su continuidad y, dependiendo de la forma en que se gestione dicho incidente, las consecuencias pueden ser más o menos graves.

Es de suma importancia conocer las consecuencias de eventos disruptivos (desastres, fallas de seguridad, pérdida del servicio y disponibilidad del servicio), las cuales se deberían someter a un análisis del impacto del negocio (BIA) del cual se habla en este documento, se puede destacar que el presente trabajo puede ser útil para implementar un plan de continuidad de negocio en

cualquier tipo de compañía o institución que posean infraestructura tecnológica y sistemas de información, Para este trabajo de investigación, la empresa Droguería y Laboratorio Henie Farma S. de R. L., sus procesos tecnológicos y equipo de usuarios clave han sido el objeto del estudio que han hecho posible la realización de la investigación y la evaluación de aplicabilidad del plan.

Los objetivos de este trabajo de investigación se concentran en evaluar el diseño e implementar un plan de continuidad del negocio, identificando los servicios tecnológicos críticos, analizando los riesgos en función de la magnitud de los daños, el período de recuperación, los tiempos máximos de interrupción y el riesgo reputacional, que ocasionaría la caída de los servicios y equipos críticos de TI, al cumplirlos se podrá garantizar un impacto positivo en la continuidad del negocio.

La estructura de esta investigación permitirá conocer el origen del problema y las soluciones adecuadas para mitigar los riesgos mediante un análisis de impacto de negocio, un amplio marco referencial basado en ITIL y COBIT dan la pauta del cómo solucionar el problema planteado; esto lleva a la ejecución de simulacros (pruebas) pre y post para evaluar los tiempos de respuesta requeridos de acuerdo con los procedimientos plasmados.

La implementación correcta del plan disminuirá la posibilidad de ocurrencia de incidentes disruptivos y, en caso de producirse, la empresa estará preparada para responder en forma adecuada y oportuna, de esa manera se reduce de manera significativa un daño potencial que pueda ser ocasionado por de los posibles incidentes relacionados a las tecnologías de la información.

Capítulo I: Planteamiento del problema

1.1 Antecedentes de la Investigación

La importancia de conocer, administrar y mantener activos los servicios y equipos tecnológicos que forman parte de la operatividad de las empresas, es de suma importancia en todas las empresas de servicios y comercialización de productos a nivel global, la dependencia de las tecnologías de aquellos procesos críticos en la producción o comercialización ha generado la necesidad por la disponibilidad de los sistemas e infraestructura tecnológica.

Uno de los principales conceptos referidos a la continuidad de los servicios críticos de TI referente a los negocios, es el de recuperación de desastres, este concepto tiene sus orígenes en las décadas de los años setenta. En aquella época, los centros de cómputo eran considerados como puntos únicos de falla y en ese sentido se desarrollaron servicios a través de los cuales diversos proveedores ofrecían acceso compartido a entornos de recuperación informática, conocidos como centro de respaldos. (Garay, 2013)

Ya en los años ochenta y noventa, este servicio adquirió mayor énfasis en el mercado, haciendo notar a las organizaciones que entre más dependencia presentaran respecto a la tecnología, mayor podría ser el impacto, en tanto no cuenten con sistemas de recuperación de infraestructura e información. Es a partir de este tipo de situaciones que las empresas analizan que las interrupciones que afecten a las tecnologías de información pueden generar pérdidas significativas, dada la fuerte dependencia de esta. (Garay, 2013)

Se pueden mencionar muchos casos a nivel internacional, en donde la disponibilidad de los sistemas se vio afectados, por ejemplo, en el atentado del 11 de septiembre del 2001, varias empresas fracasaron por la falta de medidas de respuesta a incidentes de este tipo; esto generó la necesidad de que actualmente las organizaciones estén implementando mecanismos y técnicas, que mitiguen los riesgos a los que se está expuesto, brindando una alta disponibilidad en las operaciones de su negocio. (Sánchez, 2002)

Otro caso fue el incendio de la torre Windsor en Madrid en el 2005, donde se evidenció que durante la fusión entre las compañías Andersen y Deloitte, adoptaron una serie de medidas para tener respaldo de todos los sistemas de información y de telecomunicaciones y es así cuando un periodo después ocurrió la catástrofe, que no se vio afectada en recursos humanos sino pérdidas materiales y la empresa salió a flote gracias a dichas medidas. (Mur, 2013)

A nivel empresarial, la inversión que incluya asegurar la disponibilidad de la infraestructura tecnológica en las empresas del país, son fundamentales en pocos sectores, sobre todo en el financiero, donde las normativas legales del rubro lo exigen; en este caso de investigación en donde el rubro Farmacéutico predomina, se ha evidenciado durante muchos años que las empresas que pertenecen a este, no han sido suficientemente respaldadas por una inversión económica que garantice la mitigación de los riesgos inherentes a dicha infraestructura. Esto trajo consigo la iniciativa de considerar, el estudio de riesgos de infraestructura en una empresa de este rubro. (CNBS, 2020)

En Honduras es muy común experimentar caídas en sistemas y servicios en todos los niveles y sectores, el reto de mitigar los riesgos de que estas ocurran es uno de los principales objetivos que desean alcanzar las empresas, Henie Farma pertenece al sector farmacéutico a nivel de servicio y fabricación de los productos que comercializa, esto la lleva a la necesidad de encontrar alternativas para mitigar dichos riesgos. (Redondo, 2020)

Profundizando en la empresa objeto de estudio, es importante mencionar algunas generalidades de la empresa, esto para conocer impacto negativo que una posible interrupción de la infraestructura tecnológica puede ocasionar, identificar los servicios críticos y lo que representaría para la misma una interrupción de estos.

Droguería y Laboratorio Henie Farma, en relación con sus operaciones, en sus inicios importaba los productos médicos que comercializaba, hoy en día posee una planta productora que fabrica con la marca Henie, para ubicar la empresa en el marco histórico es importante conocer la evolución del sector farmacéutico en Honduras. (Gaviria, 2004)

Según datos estadísticos conocidos, el sector de productos farmacéuticos en Honduras tiene un tamaño aparente de US\$152 millones. Esto después de experimentar una expansión superior al 300% en el año 2002. Más del 80% del mercado es atendido por productos importados, elaborados en su mayoría por empresas multinacionales, las cuales poseen fábricas en Centro América, Panamá o México. De los subsectores en estudio el que abarca mayor porcentaje del sector global es el de los medicamentos para consumo humano, seguido del subsector de medicamentos para uso animal y por último el de productos médico-quirúrgicos. (Gaviria, 2004)

En manos de estas empresas recae el proceso de registro del producto y de importación, así mismo ellas se encargan de licitar en las compras del ministerio de salud pública. Por lo tanto, se identifica que una clave para ingresar al negocio y tener éxito en el mercado es manejar una estrecha relación con al menos una de estas droguerías o distribuidoras. La comercialización minorista está dominada por tiendas independientes, bien sea farmacias o agro tiendas.

La promoción se realiza a través de visitadores médicos y de la distribución de material promocional en las farmacias. En el año 2002 el sector de productos farmacéuticos en Honduras produjo US\$30.404.895, lo que representó en el PIB del país un 0.467%. No existe información del impacto de este sector en la generación de empleo, ya que en Honduras el gobierno no posee estadísticas al respecto. (Proexport-Colombia, 2004)

Volviendo a la mención de la empresa Henie Farma, es importante estar enterado que en el año 2000 se construye el laboratorio para fabricar medicamentos propios, sumando en 2001 15 marcas y 7 genéricos, para 2018 se alcanzaron 30 marcas y 48 productos generados en el laboratorio, debido al crecimiento de la empresa y demanda de sus clientes en 2019 se realiza una expansión de procesos y modernización de maquinaria.

Para Henie Farma, la prioridad es la calidad de sus medicamentos y el bienestar de sus consumidores, buscan continuamente mejorar sus productos trabajando con proveedores certificados de reconocimiento internacional, asegurando el empaque correcto para garantizar la pureza de las moléculas, las combinaciones y formulaciones son efectivas, buscando crear sinergia y potencializar el efecto terapéutico de sus productos.

Los medicamentos en Henie Farma son producidos de forma homogénea, controlados durante todo el proceso de producción de acuerdo con lo establecido en las buenas prácticas de fabricación (BPF), para alcanzar los niveles de calidad de estándares internacionales, formulados y adecuados a su uso previsto, verificados para corresponder en su totalidad a los requisitos de autorización para ser comercializados.

Al conocer un poco sobre la operatividad de la empresa, resulta importante mencionar las dificultades operativas que afrontado la misma en los últimos años, se conoce que Honduras se ha visto afectada no solo por la pandemia que ha causado a nivel mundial enormes estragos a la salud humana y a la economía de los países, sino también se vio seriamente afectada por los huracanes eta e iota; estos pusieron a prueba la operatividad de las empresas, en Henie Farma el impacto económico negativo fue crítico los primeros meses, a pesar de no poseer una infraestructura adecuada para el trabajo desde casa, se logró mejorar los meses siguientes al cierre económico debido a los permisos de comercialización que permitieron reanudar la operabilidad del sector farmacéutico en el país.

Después de mencionar la importancia que representa Henie Farma dentro de la economía del país y las dificultades que han superado en los últimos años, es necesario estar al tanto de que posee una estructura administrativa y de producción en crecimiento continuo, con más de ochenta empleados, cuatro oficinas en tres países diferentes, una planta de producción con tecnología de punta, con equipos de TI funcionales y con todas las áreas administrativas y técnicas necesarias para la operabilidad de la empresa, se puede asegurar que los sistemas y servicios tecnológicos se volvieron fundamentales para mantener la operatividad, la regionalización también implica la necesidad de poseer lineamientos claros sobre el uso, mantenimiento e innovación de las

tecnologías de la información; sobre estas premisas se pretende mitigar los riesgos e impacto en la disponibilidad de los servicios y sistemas de información.

1.2 El problema de investigación

Enunciado

La investigación pretende encontrar las principales causas de interrupción de los servicios de TI, las cuales pueden afectar la operativa de fabricación, comercialización, facturación, y administración de la empresa, de igual forma también podría generar un impacto negativo a nivel económico o reputacional, los servicios críticos de TI de la empresa Henie Farma en la actualidad se ven seriamente amenazados, un alto grado de vulnerabilidad ante caídas o fallos en los equipos y sistemas informáticos críticos para la operación del negocio, los cuales obedecen principalmente a cortes de energía, caídas de internet y fallos en equipos críticos.

Las interrupciones en el funcionamiento de los equipos y sistemas críticos de TI podrían impactar en la:

- **Facturación de productos:** esta afecta directamente la inyección económica de la empresa, la detención de la facturación de productos puede ocasionar pérdida de la fidelidad de los clientes.
- **Generación de pedidos:** afecta directamente al área de comercialización, no contar con los servicios de generación de pedidos en línea ocasionaría retrasos en la operativa de facturación.
- **Órdenes de producción:** los equipos críticos de TI ligados al área de producción son fundamentales para fabricar los productos, el sistema de información que maneja el proceso de dichas órdenes es primordial para el manejo de inventario de

materia prima y producto terminado, una caída de estos servicios o equipos causarían serios problemas en la planta de producción.

- **Gestión del sistema contable:** una caída del sistema de información detendría la operativa administrativa, generando serios atrasos en la gestión de las cuentas por cobrar y cuentas por pagar.

Formulación

La falta de disponibilidad, integridad y accesibilidad de los servicios y equipos de TI que controlan o forman parte de la operativa de Henie Farma, es lo que enmarca el problema de investigación, sobre todo aquellos sistemas o equipos considerados indispensables para el funcionamiento de los procesos operativos críticos, las causales que podrían considerarse van desde el bajo presupuesto asignado a tecnología hasta la gestión inadecuada con proveedores, entre otros.

1.3. Preguntas de Investigación

General

- ¿Cuáles son las principales causas que podrían interrumpir la operatividad de los servicios y equipos críticos de TI en la empresa y cuál es su impacto en la continuidad del negocio?

Específicas

- ¿Cómo se ha preparado Henie Farma en estrategias de recuperación y disponibilidad de los servicios y equipos de TI, para mitigar los riesgos de interrupciones y asegurar la continuidad de las operaciones?
- Ante la caída de los servicios de TI ¿Cuáles son los tiempos de recuperación de los sistemas críticos que garantizan la operatividad de la empresa?

1.4 Objetivos de la Investigación

1.4.1 Objetivo General

- Evaluar el diseño e implementación del plan de continuidad del negocio aplicado a la Droguería y Laboratorio Henie Farma S. de R.L., Honduras.

1.4.2 Objetivos Específicos

- Identificar los servicios tecnológicos críticos del negocio necesarios para el diseño de un plan de continuidad del negocio para Henie Farma S. de R.L.
- Analizar los riesgos en función de la magnitud de los daños, período de recuperación, tiempos máximos de interrupción y el riesgo reputacional, que ocasionarían la caída de los servicios y equipos críticos de TI.
- Evaluar la efectividad de respuesta, para los tiempos de recuperación de los sistemas y equipos críticos de TI, en Henie Farma Tegucigalpa, Honduras.

1.5 Justificación del Estudio

América Latina y el Caribe es una región donde eventos naturales de gran escala han ocurrido: terremotos, tsunamis, huracanes, tormentas tropicales, incendios, inundaciones, deslizamientos de tierra, entre otros; y tanto como las poblaciones se ven afectadas, también las propias empresas se ven impactadas por estos incidentes que las obligan a paralizar sus operaciones.

Además de los factores naturales y riesgos externos, las empresas en Honduras presentan diferentes riesgos de tipo financiero, de información, operativos, entre otros; que son de carácter

interno y que podrían ser un gran problema para la continuidad del negocio; hoy en día toda organización depende de sus recursos y del personal que realiza las tareas diarias, con el fin de mantener la estabilidad de los servicios que ofrece.

La mayoría posee bienes tangibles, empleados, sistemas y tecnologías de información, etc. Si alguno de estos componentes es dañado o deja de estar accesible por la razón que sea, la organización puede paralizarse. (SELA, 2013)

Relevancia e importancia

Para el departamento de TI de Henie Farma S. de R. L. a través de su coordinación, tienen claro que aunque es normal crear una relación entre la incertidumbre y los escenarios negativos en las empresas de producción y servicio como Henie Farma, las contingencias también pueden verse como una ganancia inesperada, por ejemplo la acción sobre la operativa de crear un pedido de compra enorme o la facturación en horas pico de pedidos, atacar esos casos a fin de garantizar la disponibilidad de los sistemas sin interrupciones o fallas de hardware, son alcances necesarios para un óptimo servicio de TI.

Cualquiera sea el caso, una contingencia siempre interrumpe, de forma inesperada, la operativa normal de una empresa, es importante mencionar que, para minimizar el impacto y riesgo operativo, sobre todo en las operaciones que afectan los procesos críticos regulares de la empresa, esta debe contar con procedimientos precisos que admitan una pronta recuperación ante las fallas de los sistemas o equipos, para tener idea del grado de importancia que esto representa se pueden reflejar las posibles pérdidas económicas en relación con la operativa:

Tabla 1. Detalle de procesos críticos y su impacto económico.

Proceso	Equipos	Sistemas	Riesgo Reputa cional	Estimado en pérdidas \$ (Ventas/Producc ión por mes)	Tiempo Tolerable de Recuperación
Facturación	Servidor de aplicaciones, ruteadores, LAN	Aspel SAE	Alto	\$ 47,600	30 minutos
Comercialización	Servidor de aplicaciones, internet, ruteadores, equipos móviles	Aspel SAE Móvil, intranet.	Alto	\$ 47,600	60 minutos
Administración	Servidor de aplicaciones, ruteadores, LAN	Aspel SAE, COI, BAN	Medio	\$ 10,000	30 minutos
Producción	Equipos de embazado, etiquetado, etc.	Aspel PROD, SAE	Medio	\$ 20,000	60 minutos

Fuente: elaborado por el Investigador

Nota. Datos estimados según las ventas netas mensuales promedio, en base a una pérdida de alrededor del 7.5% mensual.

1.6 Delimitación del Problema

Se plantea como alcance, recopilar las mejores prácticas en función a cuatro referentes fundamentales para la confección de un plan de continuidad del negocio (Business Continuity Plan, BCP): (a) ISO (International Organization for Standardization) 22301:2012, (b) ISO/IEC 27005:2011, (c) ITIL 4 (Information Technology Infrastructure Library), y (d) *Good Practice Guidelines ITSM* (GPG).

Con la investigación y síntesis de esas herramientas se podrá generar una propuesta del plan de continuidad del negocio para la empresa, enfocada en los riesgos tecnológicos de esta. El proyecto del plan de continuidad del negocio es aplicable para la estructura organizacional de Henie Farma S. de R. L. Honduras, para el año 2021; con su posible incorporación en sus oficinas a nivel regional (Nicaragua y Guatemala).

Para poder delimitar la investigación es necesario identificar en el tiempo de manera retrospectiva todas las caídas en los sistemas (años 2019-2020), en los enlaces de comunicación, fallos en servidores, etc., esta información nos dará la experiencia para disminuir o desaparecer dichos fallos, acoplando ITIL al recurso tecnológico disponible y estructurar planes de acción antes posibles eventos no controlados en un futuro cercano.

La investigación se delimita geográficamente a Droguería y Laboratorio Henie Farma ubicada en Tegucigalpa, Zona Industrial Santa Bárbara, con epicentro en el departamento de TI de la misma empresa, se espera que la investigación e implementación de las propuestas se logren de 6 a 12 meses, sin olvidar la importancia de los simulacros programados, los cuales formarán parte integral del plan de continuidad y de la programación anual de las revisiones de TI.

Posibles deficiencias en el proceso de la investigación

- Una posible deficiencia del proyecto radicaría en la aplicabilidad (solución) de la propuesta, ya que depende de una fuerte inversión en infraestructura y de la autorización de la Presidencia de Henie Farma.

1.7 Viabilidad del Estudio

La propuesta de investigación está orientadas a la empresa donde actualmente labora el investigador, como responsable del departamento de TI se considera que el problema representa en la realidad, debilidades que se pretenden mitigar a largo o mediano plazo, crear un documento que defina la solución al problema será el principal objetivo de esta tesis de postgrado, desarrollar un plan de continuidad del negocio de los servicios de TI para Henie Farma S. de R. L.

1.7.1 Viabilidad Técnica-funcional

1.7.1.1 Operativa

Por el rubro de la empresa, el uso permanente de los sistemas y equipos de TI, la probabilidad de implementar un proyecto para contrarrestar problemas en la continuidad o caída de los servicios de TI son favorables, el equipo actual de TI garantizaría la operatividad de los servicios de TI, orientando y guiando a los usuarios, proveedores tecnológicos y de servicios para lograr buenos tiempos de respuesta.

1.7.1.2 Recursos Financieros

La necesidad de mantener los servicios de TI bajo un esquema de integridad, confidencialidad y disponibilidad obliga a la empresa a tomar acciones de corrección y prevención de caídas en los sistemas evitando así pérdidas económicas a raíz de parar la operatividad, por ello

se agrega al presupuesto cada año un monto de acuerdo con los proyectos venideros, de esta forma cualquier mejora o implementación para corregir las caídas en los sistemas, servidores o servicios deberá ser presupuestada

1.7.1.3 Recursos Humanos

El recurso humano de TI está capacitado para llevar a cabo este tipo de proyectos y los usuarios finales poseen la cultura de cambio respecto a tecnología.

1.7.1.4 Acceso a fuentes

El investigador menciona que como colaborador de la empresa de Henie Farma y estudiante de la maestría de gestión informática de la UNAH, se posee acceso a la documentación técnica, contactos requeridos y a la información externa sobre similares proyectos de mitigación.

Capítulo II. Fundamentos Teóricos de la Investigación

2.1 Marco Referencial

2.1.1 Requerimientos: Análisis de Impacto del Negocio

Se realizará un análisis de impacto del negocio (*Business Impact Analysis*, por sus siglas en inglés BIA) para estimar el grado de afectación que podría padecer la empresa como resultado de algún incidente o desastre. Para poder generar un análisis de impacto en el negocio de manera precisa se debe identificar el impacto de la interrupción en el negocio y determinar los requerimientos necesarios para recuperar los procesos críticos del negocio una vez ocurrido el desastre.

Respecto al análisis de impacto del negocio se desarrollarán objetivos, alcance y suposiciones, se deben identificar funciones y procesos, evaluar el impacto financiero y operacional, identificar procesos críticos del negocio, identificar y priorizar los procesos del negocio, identificar sistemas y aplicaciones críticas de TI, determinar el tiempo objetivo de recuperación, encontrar el tiempo de recuperación del trabajo, determinar el punto objetivo de recuperación y realizar un análisis del daño que causa la interrupción de un proceso. (Goh, 2015)

Para la obtención de los datos a fin de elaborar el plan de continuidad es necesario utilizar una combinación de encuestas y entrevistas, las cuales se deben realizar a personal clave de la empresa como ser los gerentes de departamento de Henie Farma S. de R.L... Se pretende utilizar un formato para catálogo de servicios; para obtener datos como: servicios soportados por TI, tiempo máximo que el departamento puede estar sin el servicio y criticidad del servicio para cada departamento evaluado, estos datos son de utilidad para el desarrollo del análisis de impacto.

2.1.2 Objetivos y Alcance del Análisis de Impacto del Negocio

El marco de acción estará basado en identificar el impacto de una interrupción en el negocio, lo cual justifica en cierta medida la adopción del plan, poder contar de manera formal y documental con los lineamientos para recuperar los procesos críticos del negocio una vez ocurrida la interrupción, brindará la pauta de la contingencia, es importante mencionar que el plan se basa en el análisis de procesos de las siguientes áreas: facturación, comercialización y producción.

El análisis de impacto que se realizará antes (simulacro #1) y después (simulacro #2) de implementar el plan, permitirá obtener información gerencial para la toma de decisiones, conocer las áreas críticas del negocio, el impacto operacional de la interrupción del negocio, las deficiencias en las capacidades actuales de recuperación. Este cumulo de datos permite la estimación del plan de continuidad, inversión y beneficios.

Alcance

El BIA que se desarrollará en este ítem está enfocado única y exclusivamente al Departamento de Tecnologías de la Información de Henie Farma S. de R.L. Se realizará el análisis del impacto que provoca un desastre y las posibles medidas que se tomarán para recuperar sistemas, recursos y datos.

2.1.3 Identificar Procesos y Funciones

- Procesos: actividades que los empleados de la empresa realizan en sus departamentos, tales como: facturación, bancos, cuentas por cobrar, etc.
- Funciones: departamentos que conforman la empresa, tales como: contabilidad, logística, TI, etc.

Los Departamentos que intervienen en el plan de continuidad son:

- Contabilidad
- Control de Calidad
- Producción
- Comercialización
- Logística
- TI
- Créditos y Cobros

2.1.4 Evaluaciones del BIA

2.1.4.1 Procesos y funciones, Henie Farma

Tabla 2. Procesos y funciones en Henie Farma.

Función del negocio	Proceso del negocio	Descripción
Contabilidad, Créditos y Cobros	Facturación	Proceso de emisión de facturas, regulado por el SAR, cuyo origen es el pedido de uno o varios productos.
	administración de cuentas por pagar y cuentas por cobrar	Las cuentas por cobrar representan el crédito que concede la empresa a sus clientes con una cuenta abierta, las cuentas por pagar son las deudas adquiridas a proveedores.
	Bancos, proveedores y clientes	Administración de transacciones bancarias, gestiones con proveedores y clientes.
	Supervisión de	Área perteneciente a producción y

Función del negocio	Proceso del negocio	Descripción
Control de Calidad	efectos de los medicamentos	desarrollo, encargada de revisar y garantizar la calidad de los productos.
	Investigación científica para nuevos medicamentos	Pruebas de desarrollo para nuevos productos.
Producción/Dirección	Legalización de productos en instituciones correspondientes	Procesos de regulación sanitaria, tributarias, etc.
	Fijación de precios de productos	Costeo de la producción de los diferentes productos.
	Alineamiento del área de registro sanitario con ARSA e instituciones internacionales	Procesos de regulación sanitaria, tributarias, etc.
Comercialización	Generación de órdenes de pedido	El cliente pide uno o varios productos al asesor comercial o visitador médico.
	Generar reporte de ventas	La gerencia comercial monitorea las estadísticas de ventas para implementar nuevas estrategias.
	Visita médica	Se encargan de presentar los productos fabricados en la empresa y sus beneficios, se relacionan con médicos y especialistas de la salud.
	Promocionar productos	Estrategias de mercadeo de los productos.
	Promover programas de apoyo para	Estrategias como: ofertas, cupones de descuento, premios, etc., orientados a

Función del negocio	Proceso del negocio	Descripción
	médicos y clientes	los clientes.
Logística	Importación de materias Primas	Adquisición de materiales y moléculas del extranjero para la fabricación de productos.
	Distribución de productos	Envío y entrega de los productos vendidos.
	Almacenamiento de productos	Manejo de los productos en las diferentes bodegas y depósitos.
	Reportes de Stock	Estadísticas de existencias del inventario.
TI	Creación de usuarios	Administración de usuarios de los sistemas.
	Backups	Respaldo de la base de datos del ERP y del servidor de archivos.
	Mantenimiento de comunicaciones	Revisiones y mantenimientos a la red de área local del edificio Henie Farma.
	Mantenimiento de hardware	Soporte preventivo y correctivo sobre equipos de cómputo.
	Mantenimiento de software	Soporte preventivo y correctivo sobre software y sistemas.
	Adquisición de equipos	Gestión de adquisición de equipo tecnológico.
	Adquisición de software	Gestión de adquisición de sistemas.
	Soporte a usuarios	Soporte técnico a usuario final.

Función del negocio	Proceso del negocio	Descripción
	Capacitación a usuarios	Jornadas de capacitación para el uso adecuado de sistemas y equipos tecnológicos.
	Administración de base de datos	Gestión de las bases de datos de los sistemas.
	Mantenimiento y soporte del ERP (ASPEL)	Revisiones y cambios en el Sistema ERP Aspel.
	Administración Web	Actualización y mantenimiento del sitio web www.henielab.com

Nota: Elaborado por el Investigador

2.1.4.2 Contexto de la Evaluación del Impacto Financiero y Operacional

La evaluación del impacto financiero y operacional asumiendo que ocurra una interrupción o desastre será evaluado mediante los indicadores del plan, los tiempos de respuesta y recuperación, darán un estimado cuantificable de las posibles pérdidas en cada uno de los casos fundamentales del estudio: proceso de facturación, comercialización y producción.

2.1.4.2.1 Contexto: Evaluación del Impacto Financiero

Para poder tener una idea clara y precisa del impacto económico es necesario antes preguntar: ¿Cuál sería el impacto de la pérdida financiera si los procesos del negocio se interrumpen por un fallo o desastre?

Para evaluar el impacto financiero se debe considerar el momento más crítico de cada función del negocio. Para el caso de investigación Henie Farma los valores se especifican de manera cualitativa, dado que no es posible obtener cifras exactas por el grado de confidencialidad que rige la empresa, a continuación, se describen los valores utilizados en pérdidas por día de ganancias por concepto de ventas, se pueden definir los siguientes rangos:

- *Impacto 0*: no hay pérdidas: 0 días
- *Impacto 1*: bajo: 1-4 días
- *Impacto 2*: medio: 5-10 días
- *Impacto 3*: alto: más de 10 días (ICONTEC, 2009)

2.1.4.2.2 Contexto: Evaluación del impacto operacional

El impacto operacional puede surgir por la alteración de los niveles normales de diferentes factores como: suficiencia del servicio prestado, eficacia del servicio, satisfacción del cliente, imagen que proyecta la compañía, confianza del cliente, control de la compañía, ética y moral, posicionamiento en el mercado, dinero circulante en la empresa, etc.

Para la evaluación del impacto operacional; se tomarán tres factores representativos y diversos para evaluar el impacto operacional: flujo de caja, satisfacción del cliente y posicionamiento en el mercado, los cuales cubren diferentes áreas de la empresa.

El impacto operacional puede ser medido con los siguientes valores:

0: no produce impacto

1: bajo impacto

2: impacto medio

3: alto impacto
(ICONTEC, 2009)

2.1.4.3 Identificar Procesos Críticos del Negocio

Para definir los procesos críticos del negocio se analizan varios criterios cuyos valores fueron evaluados en la etapa anterior. Un proceso es crítico si: el impacto financiero se tiene un valor de 2 o 3, si en el impacto operacional existen al menos dos valores “Alto” y si el impacto operacional existe al menos un valor “Alto” y un valor “Medio”. Todos estos datos referentes a las valoraciones plasmadas de los riesgos operacionales y financieros.

Si se da una valoración cuantitativa entre 0 y 3 a los indicadores del impacto operacional, de la siguiente manera:

Ninguno: 0: no produce impacto

1: Impacto Bajo

2: Impacto Medio

3: Impacto Alto: 3

Se suman los valores del impacto financiero y operacional para sacar un total que servirá para evaluar el tiempo máximo que un proceso puede estar fuera de operaciones.(ICONTEC, 2009)

2.2 Marco Teórico

El presente trabajo de investigación se enfoca en el diseño, implementación y evaluación de un plan de continuidad del negocio, que permitirá mitigar los riesgos inherentes a los servicios tecnológicos asociados a procesos operativos críticos de la empresa Henie Farma, para poder adentrarse en el tema de investigación es necesario conocer cierta terminología y datos de importancia sobre los planes de continuidad.

2.2.1 ¿Qué es un Plan de Recuperación de Desastres?

El Plan de Recuperación de Desastres (Disaster Recovery Plan, por sus siglas en inglés DRP), consiste en una serie de medidas que se toman desde un punto de vista operacional y de TI para respaldar los datos de la empresa en caso de una interrupción por el clima, piratería o error humano. (IBM, 2019)

Toda empresa necesita alguna forma de DRP. En un mundo cada vez más digital, los activos más importantes de una empresa se almacenan como datos dentro de infraestructura. Incluso un simple apagón de una hora puede causar estragos en la capacidad de su negocio para volver a funcionar sin medidas básicas de recuperación de desastres.

Las empresas necesitan establecer sus RTO (Recovery Time Objectives - Tiempo Objetivos de Recuperación) y RPO (Recovery Time Objectives - Punto Objetivo de Recuperación). Saber cuánto puede durar la empresa sin sus datos es importante porque ayuda a desarrollar un plan que sea rentable, al tiempo que cumple sus objetivos comerciales. Un buen plan de recuperación de desastres hace más que solo anticipar la pérdida de datos. Evalúa los riesgos de pérdida de datos en toda la organización dentro de cada departamento. (IBM, 2019)

Un plan de recuperación de desastres es el nivel de protección más básico que puedes aprovechar para respaldar el negocio después de que sea golpeado por un desastre, provocado por el hombre o de otra manera. (ISO.org, 2015)

Es de suma importancia entender que el DRP debe estar incluido dentro del Plan de Continuidad y que es la parte medular a nivel de los procesos de infraestructura de TI que lo conforman, no se debe igualar en términos técnicos en relación con el Plan de Continuidad del Negocio (Business Continuity Plan por sus siglas en inglés BCP).



Figura 1. Elementos del Plan de Recuperación de Desastres

Fuente: Continuidad Del Negocio, Vdbackup, Vdcontinuity, Vdcustody, (Valora Data, 2018).

2.2.2 ¿Para qué se necesita un plan de continuidad del negocio?

El principal objetivo de la planificación de la continuidad del negocio es un medio de apoyo para las organizaciones, que permita reiniciar las operaciones críticas dentro del tiempo aceptable después de una interrupción o caída de los sistemas o infraestructura asociada, a través del cual se intenta reparar problemas graves (ya sean producidas por el hombre o por la naturaleza) que tienen

un impacto sobre la efectiva ejecución de los procesos críticos de una organización. Todas las áreas críticas del negocio y las funciones de apoyo están incluidas en el proceso de planificación.

La realidad empresarial muestra una era de la información, en donde la disponibilidad ininterrumpida es esencial. Existe la posibilidad de que suceda un desastre natural, una catástrofe o una acción fraudulenta, los cuales interrumpan la posibilidad de acceso a la información afectando desfavorablemente los procesos clave del negocio. Asimismo, las exigencias del mercado, junto con un mayor nivel de dependencia de la tecnología para ejecutar los procesos del negocio evidencian la necesidad de una planificación de continuidad eficiente (López-León, 2008)

2.2.3 ¿Plan de Contingencias o Plan de Continuidad?

El Plan de Contingencia es parte integral del Plan de continuidad, es importante mencionar que los Planes de Contingencia son elaborados a nivel empresarial de forma global, involucrando todas las áreas de la empresa, este trabajo de investigación se centra en investigar y aplicar las mejores prácticas a nivel de mitigación de riesgos, para el área de Tecnología de la Información y todo lo que engloba a los procesos sistematizados.

A medida que las organizaciones dependen más y más de la tecnología, esta representa un componente clave de la mayor parte de los procesos de negocio, la disponibilidad de los servicios de TI es imprescindible para su supervivencia. Esta disponibilidad se consigue mediante la definición e implementación de un Plan de contingencia cuyo objetivo consiste en garantizar que se puede recuperar la infraestructura de TI que soporta dichos servicios dentro de los plazos y con el nivel de servicio acordado y necesario para el negocio. (Abast Systems & Solutions S.L., 2021)

En síntesis, el objetivo de un plan de contingencia y de un plan de continuidad del negocio se podría resumir en la maximización de la capacidad de mantener un nivel rentable no solo de las utilidades del negocio, sino también de su capacidad de operar de forma relativamente normal en el período transitorio entre el inicio de una catástrofe y de una reconstrucción completa y la recuperación del sistema de información que procesa.

2.2.4 En materia: Plan de Continuidad del Negocio (Bussines Continuity Plan por sus siglas en inglés BCP)

Plan de continuidad del negocio: (Bussines Continuity Plan) por sus siglas en inglés- BCP es un documento claro, conciso y detallado que especifica cómo deben actuar las personas y departamentos de la empresa (no solo TI), para responder ante una situación crítica de modo que el impacto para la empresa sea el menor posible. Otra definición interesante es la que presenta la compañía de seguridad informática ESET donde dice que un BCP debe contemplar las acciones que una empresa debe seguir para recuperar y restaurar las actividades críticas del negocio en un tiempo prudencial y de manera progresiva regresar a la normalidad; garantizando en todo momento la integridad, confidencialidad y disponibilidad de la información”. (Amaya, 2012).

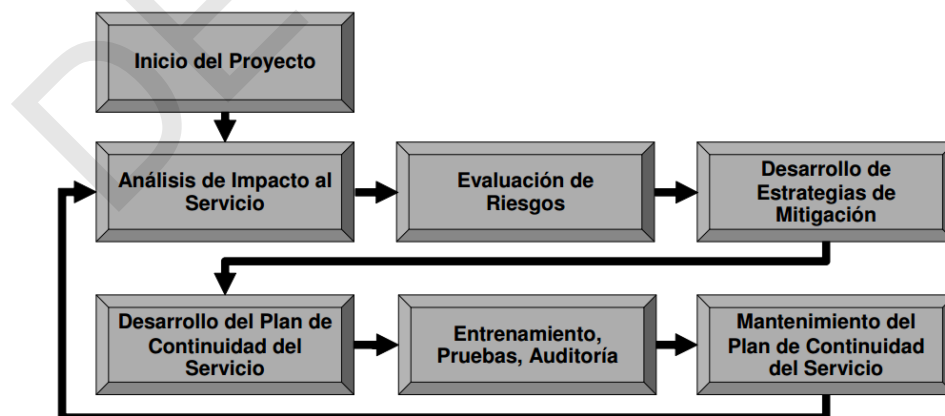


Figura 2. Estructura Plan de Continuidad del Negocio.

Fuente: SISTESEG, Planes de Continuidad del Negocio, (Ferrer, 2010).

2.2.5 Análisis de Impacto del Negocio (Business Impact Analysis por sus siglas en inglés BIA)

El propósito del BIA es crear un documento que ayude a entender el impacto que un desastre pueda tener sobre un negocio en particular. Contempla tres objetivos fundamentales: Priorizar procesos críticos del negocio. Calcular el tiempo máximo tolerable de caída (Maximum Tolerable Downtime por sus siglas en inglés MTD) el cual es el tiempo máximo sin servicio que una organización puede soportar y seguir siendo una compañía que cumple con sus objetivos de negocio.(SISTESEG, 2021)

Resumiendo lo que es el BIA, se obtiene que este pretende poner en correlación los componentes específicos del sistema con los servicios críticos que ellos proporcionan, y basado en esa información, analizar las consecuencias de una ruptura de los componentes del sistema. De igual forma pretende identificar las áreas que sufrirían las pérdidas financieras y operacionales más grandes en el caso de un desastre, además de identificar los sistemas críticos y estimar el tiempo que la compañía puede tolerar en caso de un desastre.

BIA

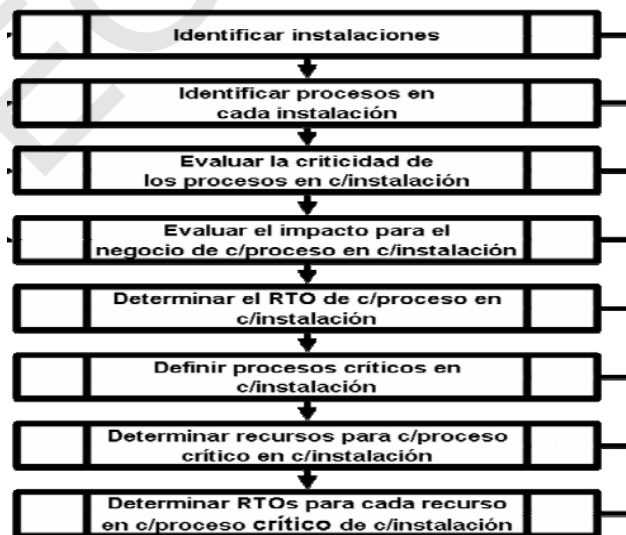


Figura 3. Ciclos del BIA

Fuente: SISTESEG, Planes de Continuidad del Negocio, (Ferrer, 2010).

2.2.6 Evaluación de riesgos

La evaluación de riesgos identifica las amenazas, vulnerabilidades y riesgos de la información, sobre la plataforma tecnológica de una organización, con el fin de generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la Información.

Los dos puntos importantes para considerar son:

- La probabilidad de una amenaza.
- La magnitud del impacto sobre el sistema, la cual se mide por el nivel de degradación de uno o combinación de alguno de los siguientes elementos: confidencialidad, disponibilidad, integridad (Ferrer, 2010).

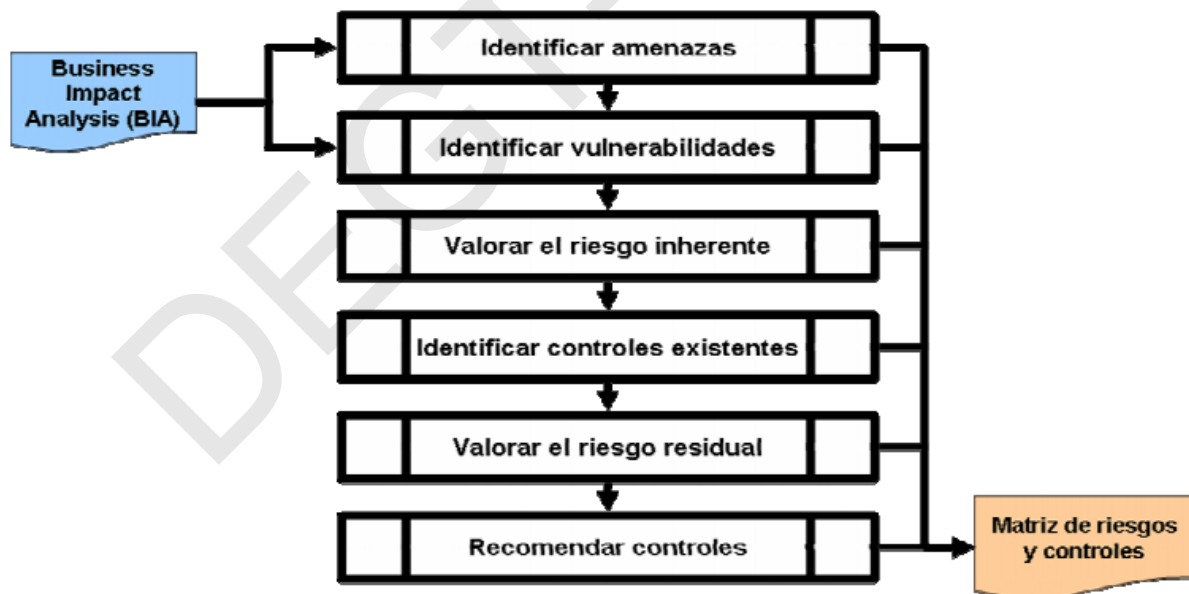


Figura 4. Gestión del Riesgo

Fuente: SISTESEG, Planes de Continuidad del Negocio, (Ferrer, 2010).

2.2.7 Plan de continuidad del negocio de acuerdo con el estándar británico BS25999.

El estándar británico BS25999, era una norma británica publicada en 2007, que rápidamente se convirtió en la norma principal para la gestión de la continuidad del negocio, fue reemplazada por ISO 22301 en 2012. Los siguientes son algunos de los procedimientos y documentos más importantes requeridos por la BS 25999-2:

- Alcance: identificación precisa de la parte de la organización en la cual se aplica la gestión de la continuidad del negocio.
- Política: definición de objetivos, responsabilidades, etc.
- Gestión de recursos humanos.
- Análisis de impactos en el negocio y evaluación de riesgos.
- Definición de estrategia de continuidad del negocio.
- Planes de continuidad del negocio.
- Mantenimiento de planes y sistemas. (Segovia, 2021)

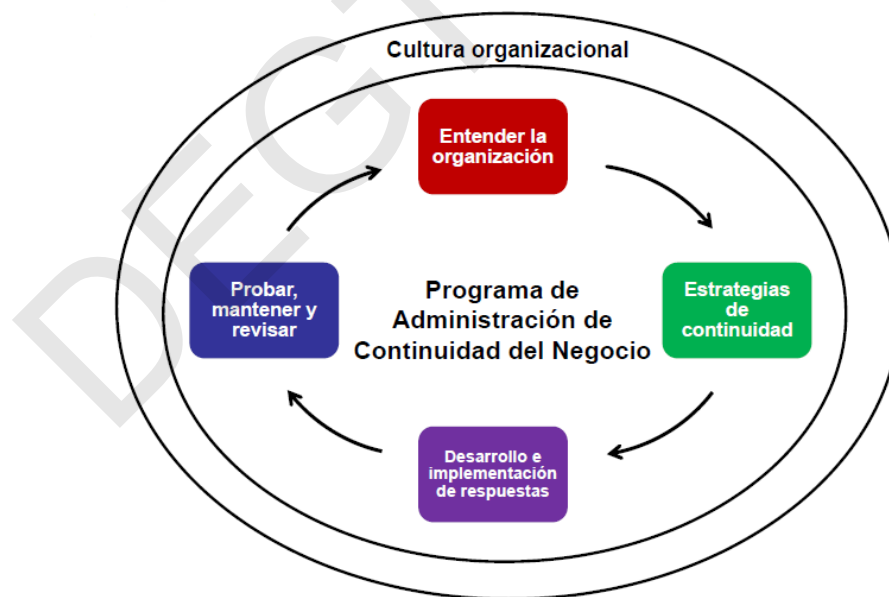


Figura 5. Proceso Metodológico según BS-25999

Fuente: (Garzón-Bejarano, 2010), *Proceso Metodológico según BS-25999*.

2.2.8 ¿Se está evaluando la Resiliencia de la infraestructura tecnológica en la empresa?

Contar con infraestructura de TI y seguridad confiable, es decir, que los involucrados sepan cómo van a reaccionar ante diversas situaciones, es indispensable. Es aquí donde entra el término resiliencia, se debe conocer la conceptualización del término en sus diferentes ámbitos.

En términos generales, resiliencia es la capacidad de un material para regresar a su forma original después de que se le ha aplicado una fuerza de deformación. En psicología, se define como la capacidad de las personas para recuperarse ante situaciones problemáticas o contratiempos y continuar con su vida.

En lo que a tecnologías de la información corresponde, resiliencia es la capacidad de la infraestructura, ya sea de seguridad o de TI, de proveer y mantener un funcionamiento aceptable a pesar de fallas y desafíos a la operación normal, por ejemplo: sobrecargas de trabajo, tráfico malicioso, etcétera.

El objetivo final es medir para cada componente aspectos como disponibilidad, rendimiento, ancho de banda, latencia, paquetes perdidos, etcétera; de tal forma que se puedan evaluar, en la vida real, qué tan resistentes son las contramedidas y tecnologías de seguridad implementadas, así como las capacidades de la infraestructura de TI con que se cuenta (Polanco, 2013).

2.3 Marco Conceptual

Para poder comprender el objetivo, alcance y los posibles resultados del Plan de Continuidad del Negocio en el desarrollo de la presente investigación, es importante conocer cierta terminología de manera conceptual:

2.3.1 Máximo Tolerable de Caídas

(Maximum Tolerable Downtimes por sus siglas en inglés MTD's)

Cuando ya se conocen los procesos críticos del negocio se define el Maximum Tolerable Downtimes (MTD). El MTD indica el tiempo máximo que un proceso del negocio puede estar fuera de servicio. (MINTIC, 2015)

Ejemplo: suponer que el proceso de gestión de nóminas no debe estar interrumpido por un periodo superior a 48h. En este caso, se establecería que el MTD asociado a dicho proceso es de 48h. (Incibe, 2017)

2.3.2 Tiempo Disponible de Recuperación

(Recovery Time Objective por sus siglas en inglés RTO)

Indica el tiempo disponible para recuperar los sistemas y recursos una vez ocurrida la interrupción. (MINTIC, 2015)

El objetivo del RTO es categorizar aplicaciones por prioridad y potencial de pérdida para ajustar los recursos en consecuencia.

Ejemplo: los planes para un RTO de casi cero requieren de servicios de conmutación por error. Uno de 4 horas permite una recuperación en sitio alcanzando una disponibilidad completa de aplicaciones y datos. Finalmente, para un RTO de 8 horas, TI suele firmar contratos con integradores de sistemas locales. (Maldonado, 2020)

2.3.3 Punto Objetivo de Recuperación

(Recovery Point Objective por sus siglas en inglés RPO)

Es importante determinar la tolerancia que tiene el negocio para la pérdida de datos como resultado de un desastre o interrupción, para esto se define el RTO. RPO (Recovery Point Objective): Es la magnitud de los datos perdidos en términos de un período de tiempo que puede ser tolerado por un proceso del negocio. (MINTIC, 2015), (Software-GreenHouse, s.f.)

Para poder generar un plan de continuidad del negocio es importante poder definir y analizar los MTD's, RTO y RPO, estos como requerimientos de los tiempos de recuperación de las operaciones en los que se debe enfocar el plan.

Ejemplo: Si se tiene un RPO de 4 horas para una aplicación, la brecha máxima entre el respaldo y la pérdida de información será de 4 horas. Esto no necesariamente significa que se perderán 4 horas de datos. Si la falla ocurre durante un momento de poca actividad, el impacto sería casi nulo; sin embargo, si esta sucede en una hora pico, la pérdida sí podría ser equivalente al tiempo de inactividad. En este caso, un respaldo más frecuente permitirá alcanzar el RPO deseado.

Dependiendo de la prioridad de cada aplicación, un RPO individual puede ir desde 25 a 12, 8, 4 horas o hasta algunos cuantos segundos. Un RPO de 8 horas puede aprovechar la solución de respaldo existente siempre y cuando tenga un impacto mínimo en los sistemas de producción. Por otro lado, un RPO de 4 horas necesita replicación instantánea. (Maldonado, 2020)

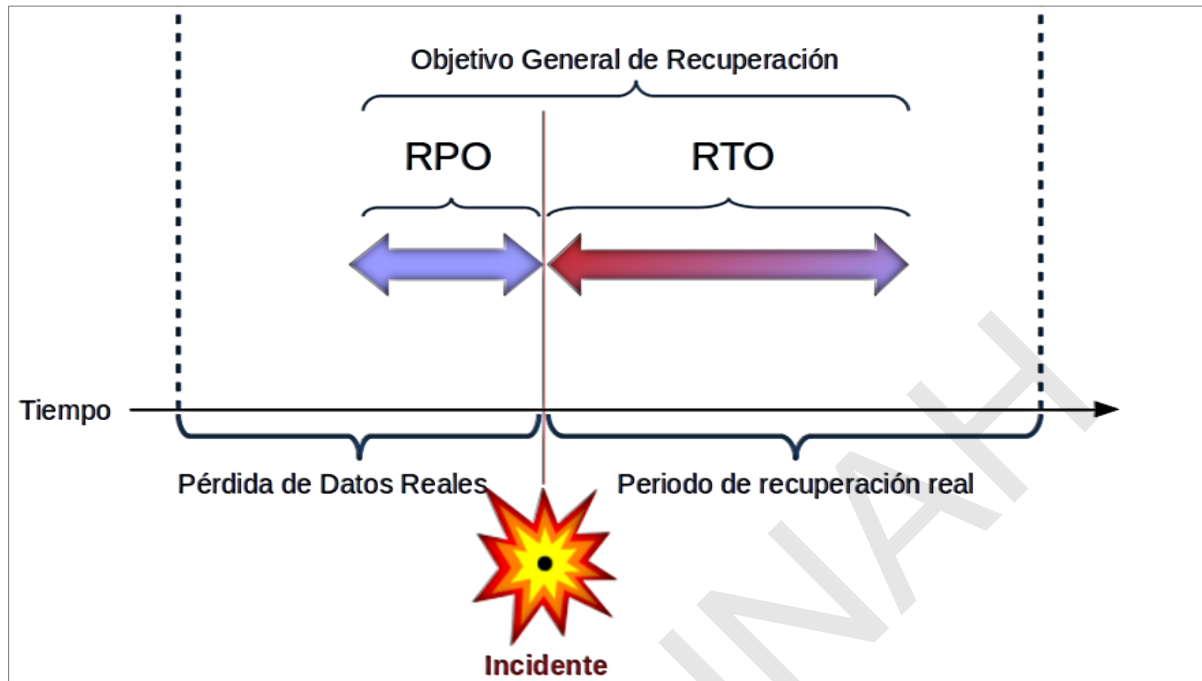


Figura 6. Objetivo general de Recuperación

Fuente: (Puricica, 2018), RTO y RPO

Evaluación de Riesgos

Identifican las amenazas de interrupción más probables y se analizan las vulnerabilidades relacionadas con dichas amenazas, evaluando los controles de seguridad física, lógica y ambiental, revisando su efectividad para contener las amenazas detectadas. (Kirvan, 2013)

Ante la eventual materialización de algún evento que ponga en riesgo la operatividad de empresa y con el fin de establecer prioridades para la mitigación de los riesgos, se hace necesario disponer de metodologías para su evaluación. En la presente investigación, a través, del plan de continuidad del negocio, se determinan los diversos escenarios de amenazas de la

empresa y los planes para reanudar los servicios que estaban en operación. La gestión del riesgo debe contemplar, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia.

Desastre

Es un evento súbito calamitoso provocado por causas naturales o humanas que conlleva consecuencias negativas como pérdidas o destrucción. (Goh, 2015).

Los desastres en el ámbito Tecnológico se consideran altamente peligrosos, hoy en día las nuevas tecnologías han sido incluidas en el manejo de operaciones o equipos para el manejo de energía nuclear, manejo de químicos, procesos industriales con alto riesgo de contaminación, etc., de igual forma es importante mencionar los desastres naturales, los cuales son comunes en Honduras debido a su ubicación geográfica, con similar grado de impacto sobre la infraestructura en general, este tipo de desastres forman parte de la difícil realidad que viven de las empresas en su día a día.

Riesgo

Es la exposición a una situación donde hay una posibilidad de sufrir un daño o de estar en peligro. Es esa vulnerabilidad o amenaza a que ocurra un evento y sus efectos sean negativos y que alguien o algo puedan verse afectados por él. Las nuevas tecnologías constituyen una red de canales multidireccionales y abiertos, así como estas ofrecen amplias posibilidades de colaboración, expresión y participación; sin embargo, el mal manejo de estas constituye un alto riesgo al nivel operativo de las empresas, el mal manejo de redes sociales, interrupción de servicios, etc., pueden provocar pérdidas considerables a nivel económico y reputacional. (Kirvan, 2013)

Vulnerabilidad

Es la condición de debilidad de una persona u organismo frente a un evento amenazante, también se entiende como la naturaleza de ser susceptible a ser dañado por no saber resistir o recuperarse ante un desastre. (Goh, 2015)

TI

Es el término abreviado para referirse a las Tecnologías de la Información: Se refiere al uso de equipos de telecomunicaciones y computadoras para la transmisión, el procesamiento y el almacenamiento de datos. La noción abarca cuestiones propias de la informática, la electrónica y las telecomunicaciones. (TechTarget, 2014)

Infraestructura tecnológica

La plataforma o infraestructura tecnológica de una organización es el conjunto de sistemas (ordenadores, equipos de electrónica de red, equipos de almacenamiento, y demás elementos físicos) junto con la manera que se ha elegido para gestionarlos (lo que incluye procesos y herramientas de gestión de los equipos, de medición de su rendimiento, de seguridad ante incidencias y catástrofes además de los sistemas operativos básicos). (CEUPE, 2021)

Data Center o Centro de Procesamiento de Datos

Es un entorno proyectado para concentrar servidores, equipo de procesamiento y almacenamiento de datos y sistemas de activos de red, como switches, enrutadores y otros. Por ello, es considerado el sistema nervioso de las empresas. (SearchDataCenter, 2009)

Centro de cableado

Es un espacio dentro de un edificio, en donde convergen todos los medios físicos de comunicación, cuyo objetivo es el transporte de datos a través una red de comunicaciones a lo largo y ancho del edificio. Dentro de la infraestructura tecnológica necesitan de otros dispositivos como switches, racks o armarios, organizadores y otros más, para interconectar varias redes. (SearchDataCenter, 2009)

Alerta

Estado declarado con el fin de tomar precauciones específicas, debido a la probable y cercana ocurrencia de un suceso adverso en la infraestructura o seguridad de los programas. (Gobierno de Alemania, 2006)

Amenaza

Peligro latente asociado con un fenómeno físico de origen natural, de origen tecnológico o provocado por el hombre que puede manifestarse en un sitio específico o en un tiempo determinado, produciendo efectos adversos en las personas, los bienes, servicios y el medio ambiente. Técnicamente se refiere a la probabilidad de ocurrencia de un evento con una cierta intensidad, en un sitio específico y en un tiempo o período determinado. (Goh, 2015)

Mitigación

Acciones que se toman para eliminar o reducir el grado de riesgo a la vida y daño a la propiedad, ya sea antes después del desastre y/o emergencia. (Gobierno de Alemania, 2006)

Control

Cualquier acción que ayude a reducir la probabilidad de ocurrencia de un riesgo o permita reducir el impacto en caso de que este ocurra. (ICONTEC, 2009)

Impacto

Se puede definir como las consecuencias para el negocio dado el daño del activo o como la evaluación del efecto o consecuencia del riesgo. Generalmente, la implicación del riesgo se mide en aspectos económicos, financieros, integridad e imagen de las personas o empresas, disminución de capacidad de respuesta y competitividad, interrupción de operaciones, entre otros. (Goh, 2015)

Probabilidad

Se puede definir como la cifra que expresa el grado de que un hecho de que sea absolutamente seguro que ocurra o no y se expresa cualitativamente como bajo, medio, alto y extremo y cuantitativamente como 0 y 1. (Khan Academy, 2021)

Proceso

Un proceso es un conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) bajo ciertas circunstancias con un fin determinado. Este término tiene significados diferentes según la rama de la ciencia o la técnica en que se utilice. (UJAEN, 2021)

Resiliencia

Este término sirve para indicar que algo puede sufrir un fallo y a pesar de ello seguir operando. Muchas veces se utiliza como si fuera un valor absoluto y, sin embargo, como sucede con los términos "cerca" o "lejos" el concepto de robustez es relativo y su alcance debe ser definido en cada utilización. Ejemplo: La duplicación del suministro eléctrico mejora la robustez o resistencia de las instalaciones frente a cortes de electricidad, pero el lugar puede volverse inservible si el fallo eléctrico afecta a ambos suministros. (Bussines Continuity Institute, 2010)

2.4 Marco Histórico Contextual

2.4.1 América Latina y el Caribe

Según estudios realizados por organizaciones sobre los Riesgos de Desastre para América Latina y el Caribe, muestran que la región es vulnerable a diferentes amenazas. "Un total de 98 desastres mayores, climáticos y geofísicos han ocurrido en América Latina y el Caribe en el año 2010 con daños superiores a los USD 49,188 millones de dólares. (SELA, 2013)

Estos datos forman parte de una tendencia regional y global que refleja el incremento de eventos desastrosos que ha hecho que el número de los desastres se haya multiplicado por cinco entre los años 1975 y 2005". Aunque los estudios sobre Reducción de Riesgos de Desastres están focalizados en evidenciar vulnerabilidades de las poblaciones, las amenazas identificadas y estudiadas se pueden tomar como referentes para aplicarlas a las organizaciones privadas o públicas. (SELA, 2013)

Una amenaza está definida como la causa potencial de un incidente no deseado y que de ocurrir puede resultar en daños a las personas, a una organización o a un sistema Una empresa u

organización no puede tener control sobre la amenaza, ésta existe por sí sola. Lo que sí puede hacer la organización es establecer medidas de protección para que en caso ocurrir la amenaza cause la mínima afectación posible. (Bussines Continuity Institute, 2010)

La continuidad del negocio y de las operaciones tiene como objetivo proteger las actividades críticas o urgentes de recuperar, y aunque pudieran resultar interrumpidas debido al incidente disruptivo, la organización será capaz de continuar brindando dichas actividades; de allí la importancia de la continuidad. (Goh, 2015)

Cuando se analizan las cifras monetarias respecto a pérdidas, resultado de desastres naturales en América latina y sobre todo Centroamérica, se observa una alta vulnerabilidad de la geografía mencionada; esto se relaciona directamente con el riesgo tecnológico y los planes de continuidad, las posibilidades de implementar respaldos en la nube, sitios alternos, redundancia en los servicios críticos, etc., pueden permitir o no a las empresas, seguir operando después de este tipo de desastres naturales, es por eso, que la implementación de un plan de continuidad de negocio se ha vuelto necesario para las empresas en crecimiento, sobre todo aquellas que ofrecen servicios o productos.

2.4.1.1 Amenazas naturales

Se pueden entender como aquellas que ocurren sin la intervención del ser humano y atribuible a un fenómeno físico de origen natural. La National Fire Protection Association (NFPA) lista estas posibles amenazas en su estándar 1600 del año 2010 de la siguiente manera:

- Geológicas: terremoto, sismo; tsunami; erupción volcánica; deslizamiento de tierras, avalanchas de lodo, hundimientos; glaciares e icebergs.
- Meteorológicas: inundación, mareas altas; sequías, hambrunas; incendios; nevadas,

heladas, granizadas y avalanchas; huracanes, tormentas tropicales, tornados, tormentas de arena; temperaturas extremas (calor o frío); rayos; tormentas geomagnéticas.

- Biológicas: enfermedades con impacto en los seres humanos o animales (peste, viruela, ántrax, virus del Nilo Occidental, fiebre aftosa, síndrome respiratorio agudo severo, enfermedades pandémicas, enfermedad de las vacas locas); infestación o daño por insectos o animales (como el dengue) (SELA, 2013)

Dependiendo de la ubicación geográfica de la organización, alguna de estas amenazas será más probable de ocurrir. Nuestra geografía regional muestra que se tiene muy al sur, tanto en Argentina como en Chile zonas de mucha nieve y hielo por lo que las avalanchas son posibles, en Chile y Perú existe una extensa franja desértica y las lluvias torrenciales son un incidente severo. La gran mayoría de los países de Latinoamérica y el Caribe tienen mares por lo que los tsunamis pueden ocurrir. (SELA, 2013)

En Centroamérica y el Caribe se tienen temporadas ciclónicas que afectan fuertemente los territorios de los diferentes países, la Cordillera de los Andes tiene aún volcanes activos; la extensa selva sudamericana y el clima tropical de muchos países de Centroamérica y El Caribe hacen propensas las lluvias, inundaciones y deslizamientos de tierra al igual que los fenómenos del niño o de la niña. Han sufrido contagios masivos por la gripe aviar H1N1 llegando inclusive a declarar cuarentena general como ocurrió en el Distrito Federal de México. En la región existen zonas remotas con enfermedades endémicas; el dengue aún es un problema no controlado. (SELA, 2013)

En los últimos años (2020-2021) la humanidad ha sufrido una pandemia que afectó no solo la salud de los individuos, la economía global sigue siendo seriamente impactada de forma negativa por dicha pandemia; al ubicarnos en la realidad local, Honduras sufrió encima de dicha

pandemia, dos huracanes que azotaron sin piedad la geografía nacional, todos estos elementos naturales mezclados con malas decisiones gubernamentales, han afectado la operación de muchas empresas que no estaban preparadas ante este tipo de eventos, detener operaciones durante tiempos prolongados ha sido el final de muchas empresas de servicios y productos, la falta de conocimiento y práctica del teletrabajo, servicios remotos, manejo de sitios alternos, disponibilidad en la nube, se consideran cruciales para que estas empresas hayan desaparecido.

Los estudios para conocer las zonas de riesgos y los potenciales desastres en la región son variados y resulta algo complejo conseguir información confiable. Algunas fuentes de información son en primer orden las propias instituciones en cada país responsable de la prevención de riesgos de desastres, también existe el Centro Regional de Información sobre Desastres (CRID), iniciativa creada para unir esfuerzos y asegurar de manera confiable la recopilación y disseminación de información disponible sobre el tema de desastres en América Latina y el Caribe; otra fuente de información son las universidades de cada país. (SELA, 2013)

Existen datos interesantes respecto a las zonas de riesgo en Honduras, la experiencia ha llevado a conocer a muchos representantes de empresas en el área tecnológica que se han basado únicamente en sitios de riesgo respecto a inundaciones, todo esto en la geografía nacional, la experiencia y nuevos estudios de riesgos tecnológicos revelan datos muy importantes a la hora de elegir por ejemplo sitios alternos, proveedores de servicios tecnológicos, ubicaciones para montar centros de datos, etc., un ejemplo claro es el de una empresa que brinda servicios tecnológicos a una amplia red de instituciones financieras a nivel nacional, tener su centro de datos en una zona geográfica donde existen más de 46 fallas geológicas es un riesgo alto, es por ello que el estudio e implementación de un plan de continuidad es fundamental para las empresas.

2.4.1.2 Amenazas causadas por el hombre

Se han catalogado estas posibles amenazas de la siguiente manera:

- a) Riesgos accidentales: derrame o escape de materiales peligrosos; explosión, incendio; accidente de transporte; colapso de edificio o estructura; falla en la red del servicio público de electricidad, gas, agua u otro similar; escasez de combustibles o de recursos; contaminación de agua o aire; falla en la estructura de contención de un dique o una presa; depresión económica, inflación, crisis financiera; interrupción en los sistemas de comunicación (voz y datos); desinformación.
- b) Riesgos intencionales: terrorismo (en sus diferentes modalidades: explosión, por sustancias químicas, biológico, radiológico, nuclear, cibernético); sabotaje; disturbio social, protestas, histeria colectiva, amotinamiento; guerra; insurrección; desinformación o rumor; actividad criminal (vandalismo, robo, incendio, fraude, malversación, robo de datos); pulso electromagnético; violación de la seguridad física o de información; violencia en el lugar de trabajo, universidad, colegio; contaminación o producto defectuoso; acoso; discriminación.

En el caso de los riesgos intencionales, estas amenazas tienen una relación directa con los problemas sociales y la región tiene mucho de ellos. En el Informe sobre Seguridad en las Américas del Observatorio Hemisférico de Seguridad de la OEA - Alertamerica.org se dan estadísticas por país sobre los principales factores de violencia social, entre ellos: homicidios y muertes violentas, tráfico de armas, consumo y comercialización de drogas, delitos de índole sexual y trata de personas, muchos de ellos asociados a una cada vez creciente red de crimen organizado. (SELA, 2013)

2.4.1.3 Amenazas causadas por fallo de la tecnología por razones no atribuibles a la naturaleza o al hombre

La asociación Nacional de Protección Contra el Fuego (National Fire Protection Association con sus siglas en inglés NFPA) clasifica estas posibles amenazas en su estándar 1600 del año 2010 de la siguiente manera: Fallos en los computadores centrales, servidores, software o aplicaciones, fallos en los equipos auxiliares de apoyo; daños en las telecomunicaciones, fallos en la energía, electricidad o servicios públicos. (NFPA, 2021)

Aunque no existen estadísticas oficiales sobre las fallas en el uso de la tecnología en las empresas de nuestra región, si resultase interesante mirar las estadísticas asociadas al uso del internet en los países de la región para darnos cuenta de cuáles son los países con mayor uso de la tecnología. De acuerdo con las estadísticas de la UIT, el acceso de internet en los hogares para Latinoamérica y el Caribe muestra a Brasil en primer orden, seguido por Chile, Argentina, Costa Rica, Uruguay, Colombia, México, y Panamá por encima del promedio de la región. (SELA, 2013)

Los datos anteriormente citados dictan una pauta importante para la creación del plan de continuidad del negocio, el análisis de riesgo sobre este tipo de amenazas: sobre todo las intencionales, deben ser parte del cumplimiento del plan, conocer las posibles formas en que los usuarios internos o externos pueden causar un fallo o interrupción en los servicios críticos del negocio, es de sumo interés; por todo esto se deben considerar las soluciones o controles para mitigar estas acciones intencionales.

2.4.2 Contexto Nacional

A raíz de muchas catástrofes naturales Honduras es parte de las naciones más golpeadas por los fenómenos naturales como las tormentas tropicales y los huracanes, estas provocan comúnmente inundaciones en todo el territorio nacional, los temas de continuidad de negocio y de recuperación ante desastres son cada vez más importantes para el sector empresarial, sobre todo el privado; contar con un plan de continuidad de las operaciones se ha vuelto una necesidad.

Ante la situación expresada u observada previamente, las inversiones tecnológicas se están volviendo cada vez más necesarias en las diferentes empresas de cualquier rubro, sin embargo, el sector Financiero es el único regulado para dichos fines.

2.5 Marco Legal

En la actualidad no existe un marco legal que regule u obligue a la empresa privada o gubernamental a desarrollar un plan de continuidad de negocio y garantizar los servicios que ofrecen, la única institución que posee una regulación es la Comisión Nacional de Banca y Seguros y su alcance llega solo al sector financiero del país, las circulares con un contenido basto en temas de continuidad de negocio son la Circular 119/2005 y El Proyecto de Reforma a la Norma de Gestión del Riesgo Operativo, ambos descritos en sus apartados referentes a continuación.

2.5.1 Circular CNBS No.119/2005

La Comisión Nacional de Banca y Seguros CNBS en su CIRCULAR CNBS No.119/2005: Normas para regular la administración de las tecnologías de información y comunicaciones en las instituciones del sistema financiero, informa:

Que las instituciones del sistema financiero podrán ofrecer y prestar todos los productos y servicios por medios electrónicos; así como que la Comisión emitirá normas de carácter general para regular las operaciones que efectúen y servicios que presten las instituciones por medios electrónicos. (CNBS, 2005)

Y que conforme lo establecido en la Ley de la Comisión Nacional de Bancos y Seguros, ésta se encuentra sujeta a ciertos criterios, entre los cuales se señala el de promover la adopción de buenas prácticas en la administración de los riesgos inherentes a las actividades que realizan las instituciones supervisadas. (CNBS, 2005)

Dichas normas, tienen por objeto regular la administración de las tecnologías de información y comunicaciones utilizadas por las instituciones del sistema financiero; asimismo, regular los servicios financieros y operaciones realizadas por medio de redes electrónicas de uso externo e interno. (CNBS, 2005)

Las presentes normas están en concordancia con los principios del Comité de Basilea y el estándar internacional ISO/IEC 17799:2000, emitidos en materia de banca electrónica y administración de la Seguridad Informática y constituyen una guía general para la documentación formal e implementación de la seguridad en las tecnologías de información y comunicaciones de las instituciones del sistema financiero. (CNBS, 2005)

Plan De Continuidad Del Negocio, Sección Única

Artículo 36.- Plan de Contingencias

- La institución deberá mantener un plan de contingencias detallado para recuperar y operar su tecnología de información en los casos de mal funcionamiento y desastres.

- La institución deberá examinar y revisar su plan de contingencias atendiendo los cambios que han ocurrido desde la revisión anterior. Dicha revisión deberá realizarse como mínimo cada dos (2) años, así como cada vez que ocurran cambios significativos.
- Asimismo, al menos anualmente y cuando ocurran cambios significativos, la institución deberá realizar y documentar pruebas de sus procesos de respaldo y recuperación.
- Los equipos de almacenamiento de los respaldos de información o los respaldos en sí deberán estar localizados en un lugar distante y distinto en donde se generó la copia de la información original.
- La institución deberá tomar las medidas que aseguren la posibilidad de reconstruir la información, tanto de las copias de respaldo, como de la información retenida en medios que ya no son utilizados. (CNBS, 2005)

2.5.2 Proyecto De Reformas A La Norma De Gestión De Riesgo Operativo

Capítulo IV. De la gestión de la continuidad de negocio y de la seguridad de la información

La gestión de la continuidad del negocio requiere que el Directorio y todo el personal de la institución, implemente un proceso que brinde respuestas efectivas para que la operatividad del negocio continúe de una manera razonable, salvaguardando los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la institución. (CNBS, 2019)

Etapas De La Gestión De Continuidad Del Negocio

Para la gestión de la continuidad del negocio, las instituciones deben considerar al menos las siguientes etapas:

a) **Análisis y Evaluación de la Continuidad del Negocio:** Las instituciones deben identificar los riesgos que podrían causar una interrupción del negocio. Una vez identificados, se debe determinar el impacto que tendría una interrupción de los procesos que soportan los principales productos y servicios. Para ello, deben considerarse aspectos como: daños a la viabilidad financiera, daños a su reputación, incumplimiento de requerimientos regulatorios, daños al personal o al público en general. Según ello, deben establecer el período máximo tolerable de interrupción (RPO) y el tiempo objetivo de recuperación (RTO) por cada uno de estos procesos. Adicionalmente, deben definir qué procesos requieren contar con una estrategia de continuidad de negocios, considerando los resultados del análisis de impacto y de la evaluación de riesgos. (CNBS, 2019)

b) **Definición de la Estrategia de Continuidad del Negocio:** Las instituciones deben determinar la estrategia de continuidad que les permitirán mantener sus actividades y procesos de negocio, luego de ocurrido un evento de interrupción de operaciones, dentro del tiempo objetivo de recuperación definido para cada proceso. La estrategia de continuidad, dependiendo del tipo de proceso que se trate, debe considerar al menos lo siguiente: seguridad del personal, habilidades y conocimientos asociados al proceso, instalaciones alternas de trabajo, infraestructura alterna de tecnología de información que soporte el proceso, seguridad de la información y equipamiento necesario para el proceso, entre otros. (CNBS, 2019)

c) **Desarrollo e implementación de la estrategia de continuidad:** Las instituciones deberán desarrollar planes de respuesta ante los eventos analizados anteriormente, e implementar un

modelo de respuesta adecuado que permita cubrir los eventos inesperados y proveer los recursos necesarios, acorde con la estrategia seleccionada, para enfrentar con éxito un evento de interrupción de operaciones. Para este fin, deben implementar un Plan de Continuidad de Negocio, el cual consiste en establecer un plan documentado que permita dotar a la institución de la capacidad de mantener, o de ser el caso recuperar, los principales procesos de negocio dentro de los parámetros previamente establecidos. (CNBS, 2019)

2.6 Marco Normativo

La normativa en seguridad informática tiene como fin de cuidar los datos e información personal de los usuarios y clientes, así como la regulación de la forma en que las organizaciones utilizan y tratan la información de los usuarios. (IsoTools, 2021)

En la mayoría de los entes regulatorios y compañías que brindan marcos de gestión, guías de buenas prácticas y metodologías para el desarrollo de planes de continuidad de negocio, entre las más importantes y reconocidas están las siguientes: (IsoTools, 2021)

2.6.1 ISO 27001

Esta norma que hace parte de la familia de las IS 27000, la cual es una norma que brinda la capacidad de garantizar la confidencialidad e integridad de los datos y de la información para las organizaciones, así como los procesos de los sistemas que las procesan, esta norma o estándar es brinda el sistema de gestión de la seguridad de la información está en especial permite a la organización la evaluación del riesgo y la aplicación de los controles necesarios para su erradicación o mitigación. Esta norma ofrece herramientas que ayudan a la implementación y desarrollo de los planes de continuidad, así como algunos pasos a seguir en caso de incidentes de seguridad. (ISOTools, 2021)

2.6.2 ISO 22301

Esta norma de la ISO está especializada en la gestión de Continuidad del Negocio creada por especialistas en el tema la cual proporciona un marco de referencia para la gestión de la continuidad de negocio en las organizaciones. Especifica los requisitos para la protección, así como para reducir los tiempos de interrupción, garantizar a la organización que se recupere de incidentes, ayuda a la identificación y gestión de las amenazas a las que se encuentra expuesta la organización, minimizar los impactos que generan los incidentes, minimizando el tiempo de inactividad causado por un incidente y reduce el tiempo de recuperación de sus procesos y servicios a su normalidad generando una imagen confiable para empleados, proveedores y usuarios. (ISO Tools, 2021)

2.6.3 COBIT

“Objetivos de Control para Información y Tecnologías Relacionadas” Cobit es un marco de buenas prácticas reconocido a nivel internacional para la gestión y control de la información en sistemas de TI, este marco se enfoca también en el gobierno de TI, objetivos de control, medidas de desempeño, contingencia, aspectos críticos de éxito y modelos de madurez, el marco de COBIT es una herramienta más que ayuda a tener un adecuado enfoque en la creación desarrollo e implementación de un plan de continuidad Cobit tiene 4 divisiones o dominios y en especial en su apartado DS4, hace referencia a objetivos de control específicos que aseguran la continuidad del negocio y de las operaciones de una organización. (Isaca.Org, 2021)

2.6.4 ITIL

“La biblioteca de infraestructura de TI” brinda un marco para la gestión de servicios de TI en cuanto a la planificación, aprovisionamiento, diseño, implementación, operación, soporte y mejora de los servicios de TI adecuados para las necesidades del negocio. ITIL proporciona un marco integral, consistente y coherente de buenas prácticas en la gestión de los servicios de TI y otros procesos relacionados. Dentro de sus objetivos de control se encuentran algunos que brinda apoyo a la continuidad de servicios de TI y disponibilidad de los servicios que en conjunto con otras normas y guías son de gran ayuda para el desarrollo de un BCP. Aunque esta guía no entra en detalles de los procesos ni como se deben hacer, si brinda procesos básicos de gestión para el desarrollo y control. (SearchDataCenter, 2009)

2.6.5 NIST SP 800-34

El Instituto nacional de Estándares y Tecnologías NIST brinda un documento guía con la cual brinda a las organizaciones a comprender el propósito, proceso y un formato del desarrollo de planes de contingencia de los sistemas de información a través de directrices y practicas reales. Además, proporciona información de antecedentes sobre las interrelaciones entre la planificación de contingencias del sistema de información y otros tipos de planes de contingencia relacionados con la seguridad y la gestión de emergencias, la capacidad de recuperación de la organización y el ciclo de vida del desarrollo del sistema de contingencia. (NIST, 2021)

2.7 Marco Institucional

Henie Farma pertenece al sector privado, es catalogada como Droguería y Laboratorio, tiene su ubicación principal en Tegucigalpa, Honduras y sus oficinas representadas en Nicaragua y Guatemala, esto le lleva a tener presencia en todo el territorio de estos tres países, mediante la representación de su visita médica y equipo de comercialización. Cuenta con un total de 68 empleados en los tres países, las divisiones operativas de Henie Farma son catalogadas como:

- Producción y Logística
- Administración
- Comercialización

En seguida se menciona una breve descripción de la situación actual y lo que se espera lograr con la aplicación del Plan de Continuidad del Negocio, en el departamento de TI de Droguería y Laboratorio Henie Farma.

Situación Actual (TI)

El área de Tecnologías de la Información es gestionada por el Gerente de TI, con sede en Tegucigalpa, Honduras, desde la cual se brinda soporte vía remota a los usuarios de Nicaragua y Guatemala.

Las políticas informáticas se manejan de forma global, sin embargo, se deben readecuar según las necesidades y leyes de cada país. Se pueden mencionar las siguientes actividades como las más importantes que se realizan en el departamento de TI: mantenimiento de telecomunicaciones, soporte usuario final, soporte al ERP, adquisición de software y equipos, administración de base de datos y administración del sitio web.

En relación con el tema de continuidad de negocio, la actualidad de Henie Farma es una gran oportunidad de mejora, ya que no cuentan con ciertos aspectos básicos que este exige, esto lleva a plantear lo que se espera lograr con la implementación del plan de continuidad del negocio (Business Continuity Plan por sus siglas en inglés BCP).

Lo que se Espera

Basado en los estándares internacionales aplicables al tema de Continuidad de Negocio de las Tecnologías de la información, se ha comenzado un trabajo arduo para mejorar la estructura del departamento de tecnología, cuya reestructuración es reciente; el objetivo es contar con personal de experiencia para llevar a Henie Farma a formar parte de la era digital, el plan de continuidad de negocio puede garantizar una mejor gestión y control de todos los procesos tecnológicos de la empresa, a fin de mantener de manera proactiva todos los sistemas e infraestructura de Henie Farma en línea.

Conocer a profundidad los escenarios de riesgo, las principales operaciones, recursos existentes, personas involucradas y el alcance del plan, permitirán a Henie Farma planificar y describir la capacidad para respuestas rápidas, requerida para el control de emergencias. Es importante saber que junto al plan se debe identificar los distintos tipos de riesgos que potencialmente podrían ocurrir e incorporar una estrategia de respuesta para cada uno.

Se podrá disponer de un procedimiento formal y por escrito que indique las acciones a seguir frente a determinados riesgos, optimizar el uso de recursos humanos y materiales y un control adecuado para cumplir con las normas y procedimientos establecidos, los planes de contingencia son necesarios en todo sistema y no podría dejarse de lado en el tema de seguridad.

Se evaluarán las cinco etapas del plan de continuidad del negocio:

- 1.- Evaluación
- 2.- Planificación
- 3.- Pruebas de viabilidad
- 4.- Ejecución
- 5.- Recuperación

Las tres primeras etapas hacen referencia al componente preventivo y las últimas a la ejecución del plan una vez ocurrido el siniestro, queda claro que lo único que permite que una institución, empresa o persona pueda reaccionar de manera adecuada ante una crisis de seguridad, es mediante la elaboración, prueba y mantenimiento de un plan de continuidad del negocio.

Capítulo III. Metodología

Los enfoques cuantitativo, cualitativo y mixto constituyen rutas posibles para resolver problemas de investigación. Todos resultan igualmente valiosos y son, hasta ahora, los mejores métodos para investigar y generar conocimientos. (Hernández-Sampieri, 2018).

A continuación, se describe la metodología utilizada en el presente trabajo de investigación:

3.1 Enfoque de investigación

La presente investigación se basa en un enfoque cuantitativo de acuerdo con (Roberto Hernández Sampieri, 2014) donde se define que dicho enfoque está organizado de manera secuencial para poder comprobar ciertas suposiciones. Las fases son precedentes y es difícil eludir alguna de ellas, el orden es riguroso, aunque con cierta flexibilidad para redefinir alguna etapa. Este enfoque parte de una idea que se delimita, se generan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o perspectiva teórica. De las preguntas se derivan hipótesis y determinan y definen variables, se seleccionan casos o unidades para medir en estas las variables en un contexto específico (lugar y tiempo); se analizan y vinculan las mediciones obtenidas (utilizando métodos estadísticos), y se extrae una serie de conclusiones respecto de la o las hipótesis. (Hernández-Sampieri, 2018)

En este sentido, esta investigación propone evaluar el diseño e implementación de un plan de continuidad del negocio para Droguería y Laboratorios Henie Farma S. de R. L. basado principalmente de ISO 22301 y estándares como ITIL V4, ITSM, ISO 27005, todo ello para que se garantice la operatividad de los sistemas e infraestructura tecnológica, ligada a la producción y comercialización de los productos que Henie Farma ofrece a sus clientes.

3.2 Tipo de Investigación

En congruencia con el enfoque cuantitativo del que se deriva la investigación, el tipo de investigación a considerar es el correlacional, ya que pretende medir el grado de relación existente entre dos o más conceptos o variables. (Roberto Hernández Sampieri, 2014)

Puede ser importante conocer que según otros autores esta investigación se considere aplicada, ya que según (Tamayo, 2002) la forma de investigación aplicada se le denomina también activa o dinámica, se encuentra íntimamente ligada a la pura ya que depende de sus descubrimientos y aportes teóricos; es el estudio o aplicación de la investigación a problemas concretos, por lo cual esta investigación se relaciona a dicho tipo de investigación al buscar resolver necesidades específicas.

3.3 Diseño de Investigación

Tomando en cuenta las posibilidades de aplicación de dichos de los resultados obtenidos de la investigación en el tiempo conveniente para Henie Farma, se describe el tipo de investigación cuantitativa de tipo correlacional transversal, todo esto a fin de describir, analizar y comprobar la metodología propuesta para la continuidad del negocio, determinando la causa y efecto de las acciones o fenómenos involucrados que se derivan del riesgo tecnológico de los servicios críticos en la operativa de la empresa.

Todo esto lleva a realizar simulacros y provocar eventos relacionados con los sistema e infraestructura crítica del negocio, con el fin de poder medir los tiempos de respuesta y de recuperación ante fallos o desastres, estos datos ayudarán a tomar decisiones acertadas sobre mitigación de riesgos inherentes a la tecnología asociada a los procesos críticos del negocio; el plan de continuidad del negocio es de hecho la propuesta de prevención, reacción y mitigación de los riesgos asociados a la continuidad de las operaciones de Henie Farma.

3.4 Población y Muestra

La población corresponde al total de usuarios que se beneficiarán con la implementación de un plan de continuidad (correspondientes a 4 oficinas) en Henie Farma S. de R. L. las cuales forman parte de las siguientes ubicaciones: Oficina Tegucigalpa (edificio central), Oficina San Pedro Sula, Oficina Managua y Oficina Ciudad de Guatemala, sin embargo, para esta investigación se eligen solo usuarios de la oficina Henie Tegucigalpa (donde radican los servicios críticos) que son clave y que utilizan los diferentes sistemas e infraestructura necesaria para mantener activa la producción y comercialización de los productos que ofrece la empresa, serán parte de la muestra elegida.

Se podrán incluir a fin de recolección de información, elementos como usuarios administrativos y los diferentes servicios, equipos o sistemas críticos en la operativa esencial del negocio, tales como: enlaces de internet, servidores, ERP Aspel, entre otros. Los procesos operativos de producción, comercialización y facturación brindarán información crucial para el desarrollo del plan.

Tabla 3. Población: usuarios que utilizan servicios de TI por país.

Población	Número de Usuarios	Porcentaje
Oficina Henie Tegucigalpa	18	58 %
Oficina Henie San Pedro Sula	5	16 %
Oficina Henie Managua	5	16 %
Oficina Henie Guatemala	3	10 %
TOTAL	31	100%

Fuente: Elaborado por el Investigador

3.4.1 Tipo de muestreo.

Para la investigación a realizar se utilizará un muestreo discrecional, también conocido como muestreo por juicio o intencional, mediante esta técnica se elegirán los usuarios de áreas específicas, aquellos usuarios claves que resulten más adecuados para obtener la información necesaria para su análisis posterior.

A efectos de validar la propuesta, se empleará una muestra no probabilística de tipo dirigida, la cual corresponde a la oficina principal de Henie Farma Tegucigalpa, incluyendo la recolección de información con apoyo de los responsables de las áreas operativa, administrativa y comercial relacionadas a los procesos críticos del negocio, en este caso de estudio los datos informativos para el análisis se obtendrán mediante técnicas e instrumentos de recopilación de información aplicados a los diferentes usuarios, entre líderes y operativos de cada área.

3.4.2 Cálculo de la muestra.

Según la población, muestra y el tipo de muestreo utilizados no es recomendable generar selección aleatoria de la muestra, para el muestreo intencional no es correcto calcular en base a un posible margen de error o nivel de confianza (Ochoa, Citado en 2021), en este caso se acompaña junto a los resultados una descripción que como y en base a que se obtuvo la muestra, para este caso los usuarios claves de las áreas involucradas de la oficina Henie Farma Tegucigalpa, que es donde radican los servicios y áreas claves son la muestra elegida.

Muestra: Usuarios Claves de Oficina Henie Farma Tegucigalpa**Tabla 4.** Población: usuarios que utilizan servicios de TI en Oficina Tegucigalpa.

Población	Número de Usuarios	Porcentaje
Finanzas	2	25 %
Facturación	1	12.5 %
Créditos y Cobros	1	12.5 %
Logística y Producción	2	25 %
Control de Calidad	2	25 %
Total, de la muestra	8	100%

Fuente: Elaborado por el Investigador

3.5 Instrumentos y Técnicas de Recolección de Información**3.5.1 Técnicas de Recolección de Información**

Como se menciona en el apartado de muestreo, para esta investigación se utilizarán dos métodos de recolección de información: el muestreo discrecional, también conocido como muestreo por juicio o intencional, mediante esta técnica se elegirán los usuarios de áreas específicas, aquellos usuarios claves que resulten más adecuados para obtener la información necesaria para su análisis posterior y la entrevista estructurada, la cual permitirá establecer una evaluación preliminar del plan de continuidad, esta es una técnica para recoger datos directamente de los participantes, que ayuda en la adquisición de información de calidad, ya que ofrece la

posibilidad de hacer preguntas detalladas y de sondear más a fondo para recopilar datos ricos e informativos. (QuestionPro, 2021)

La experiencia que se obtendrá de cada simulacro permitirá recolectar información importante sobre la experiencia de usuarios claves y del equipo de TI, a fin de mejorar o recomendar cambios en la propuesta y sobre todo en las acciones que requieren los simulacros, se realizarán preguntas generales sobre la realización de cada simulacro y se documentarán en un “Forms” de Office 365.

3.5.2 Instrumentos de Recolección de Información

Para obtener información preliminar del plan de continuidad, se deben realizar Entrevistas Estructuradas con la muestra previamente seleccionada: gerente de ti, gerente de operaciones, gerente de producción, gerente financiero; se utilizarán como instrumentos de recolección de información: listas de cotejo para obtener información previa sobre el plan de continuidad y registros (Plantillas) para recopilar información sobre los simulacros del plan.

Ver Anexo 3: Instrumentos de Recolección de Información.



La recolección de información incluye una serie de plantillas de Registro, se utilizarán diversos “Forms” de Office 365 para plasmar la información crucial del plan de continuidad: como la definición de los equipos de trabajo, de los procedimientos para determinar los tiempos críticos, valoración de impacto y recursos; de igual forma se incluirán plantillas para registrar los resultados de la activación, recuperación, restauración respecto a las pruebas (simulacros) del plan.

3.5.2.1 Evaluación Preliminar del Plan de Continuidad del Negocio

Tiene como objetivo conocer el estado del Plan de Continuidad (conocimiento previo de los usuarios clave y personal de TI), se pretende conocer la documentación existente, los escenarios previstos, funciones, recursos, sitios alternos y tiempos estimados de recuperación de las operaciones críticas del negocio.

3.5.2.2 Plantilla para registrar la Conformación de Equipos

Con la información personal de cada una de las personas que pertenecen al grupo de usuarios claves en el desarrollo y pruebas del Plan de Continuidad.

3.5.2.3 Lista de Chequeo de Notificaciones

Registros informativos respecto a los responsables e involucrados en conocer las acciones derivadas del plan de continuidad.

3.5.2.4 Lista de Chequeo de Respuesta

Registros previos de las acciones ante un eventual evento de emergencia.

3.5.2.5 Evaluación de Análisis de Impacto del Negocio (BIA)

El objetivo es recolectar la información relacionada con los procesos críticos de la empresa.

- **Tiempos Críticos**

Permitirá recolectar información de los tiempos críticos de los procesos investigados, cuando las operaciones se demandan en mayor cantidad por los usuarios.

- **Valoración del Impacto**

Se pretende determinar el impacto financiero, operacional y reputacional que la indisponibilidad de los servicios críticos causa a la empresa.

- **Planes alternos de operación**

Para identificar las actividades de un posible plan alternativo de operación establecido y probado por la gerencia Operativa. **Ver Anexo 3.**



3.5.2.6 Plantilla de Activación, Recuperación y Restauración del Plan

Se utilizarán en las pruebas que se desarrollen para el Plan de continuidad de Negocio, las actividades que se identifican se deben desarrollar en su totalidad e ir documentado en el formato los resultados obtenidos. **Ver Anexo 3**



3.5.2.7 Plantilla de Pruebas de los Simulacros

Se utiliza para dejar registro de las pruebas realizadas sobre el plan de continuidad de negocios, se deben registrar los datos de la prueba, incluyendo las actividades a realizar, los objetivos de estas, los responsables de cada actividad y la verificación de su realización. Finalmente, se debe dejar registro de los resultados de las actividades ejecutadas a lo largo de la prueba, incluyendo los tiempos utilizados y, en caso de ser necesario, los criterios de cancelación.

Ver Anexo 3 y 4



3.5.2.8 Plantilla de Experiencia del usuario posterior a los simulacros

La experiencia que se obtendrá de cada simulacro permitirá recolectar información importante sobre la experiencia de usuarios claves y del equipo de TI, a fin de mejorar o recomendar cambios en la propuesta y sobre todo en las acciones que requieren los simulacros, se realizarán preguntas generales sobre la realización de cada simulacro y se documentarán en un “Forms” de Office 365.

Ver Anexo 3



3.5.3 Proceso de Validación de Instrumentos y Técnicas

Es importante saber que la validez se refiere al grado en que un instrumento, en este caso las listas y registros formalizados, miden las variables que se buscan medir (ejecución del plan de continuidad y disponibilidad de los servicios críticos TI), para lo cual existirán dos tipos de evidencia: relacionada con el contenido de la investigación y con el criterio (Hernandez, 2010).

En este caso en particular se considerará una validez de contenido y criterio, mediante una evaluación realizada por los usuarios claves de los procesos y servicios críticos de TI, dos expertos en metodología de la investigación de la UNAH, el asesor temático y se pretende involucrar al menos un experto en el tema de continuidad del negocio (externo), quienes proporcionarán recomendaciones en cuanto a la redacción de los ítems, a fin de lograr que los instrumentos gocen de validez, buscando que estos muestren coherencia, relevancia y posean una redacción sencilla.

Para este trabajo de investigación se considerará el Coeficiente alfa de Cronbach, desarrollado por J. L. Cronbach, ya que requiere una sola administración del instrumento a un grupo de referencia, para luego realizar los cálculos correspondientes. En este sentido será necesaria la realización de una prueba piloto de los instrumentos a un número reducido de personas (5 usuarios), y mediante el empleo del paquete estadístico llamado MiniTab.

3.6 Plan de Análisis

Es importante mencionar que todos los instrumentos serán validados por los especialistas anteriormente mencionados, sin embargo, como según la descripción de cada instrumento, el plan de análisis según su origen será validado y revisado por:

Usuarios Claves de la empresa:

- Evaluación Preliminar del Plan de Continuidad del Negocio
- Plantilla para registrar la Conformación de Equipos
- Evaluación de Análisis de Impacto del Negocio (BIA)e
 - Tiempos Críticos
 - Valoración del Impacto
 - Planes alternos de operación

Experto de TI:

- Lista de Chequeo de Notificaciones
- Lista de Chequeo de Respuesta
- Plantilla de Activación, Recuperación y Restauración del Plan
- Plantilla de Pruebas de los Simulacros

La información recopilada en las listas y registros serán analizadas y tabuladas mediante la aplicación MiniTab.

3.6.1 Métodos y modelos de análisis de datos.

Se utilizará el análisis de componentes principales (ACP), la cual es una técnica utilizada para describir un conjunto de datos en términos de nuevas variables (componentes) no correlacionadas. Los componentes se ordenan por la cantidad de varianza original que describen, por lo que la técnica es útil para reducir la dimensionalidad de un conjunto de datos.

Técnicamente, el ACP busca la proyección según la cual los datos queden mejor representados en términos de mínimos cuadrados. Esta convierte un conjunto de observaciones de variables posiblemente correlacionadas en un conjunto de valores de variables sin correlación lineal llamadas componentes principales. (Colina & Roldán, 1991)

3.6.2 Programas por utilizar para análisis de datos.

Se utilizará el software llamado “R” para el análisis estadístico de los datos obtenidos, R es un lenguaje de programación y un entorno para el análisis estadístico y gráfico, es parte del sistema GNU y se distribuye bajo la licencia GNU GPL; es decir, es **software libre** y gratuito.

El programa es multiplataforma, fue inicialmente creado por R. Ihaka y R. Gentleman de la Universidad de Auckland en 1993, pero actualmente, el entorno R es el resultado de la colaboración de toda una comunidad de usuarios, a partir de 1997 el desarrollo del código fuente (o R-base) de R es llevado por un grupo de programadores conocido como “The R-core team” (Serrano, 2021).

Se utilizará para validar la hipótesis el software MiniTab, el cual es una herramienta de análisis de datos potente y de gran reputación con una interfaz intuitiva y fácil de usar tanto para usuarios nuevos como experimentados. (UCESI, 2020)

3.7. Operacionalización de Variables

Variable independiente: Plan de Continuidad de Negocio

Tabla 5. Operacionalización de la variable independiente.

Variable	Definición Conceptual	Indicadores	Sub-Indicador
Ejecución del Plan de Continuidad del Negocio	“Es un plan de emergencia con el objetivo de determinar los procesos críticos que afectarían el funcionamiento de los sistemas de información y comunicación de una organización a un nivel mínimo aceptable durante una contingencia” (Goh, 2015)	Tiempo máximo tolerable de caída de los servicios críticos (Maximun Tolerable Downtime por sus siglas en inglés MTD).	
		Tiempo Objetivo de Recuperación RTO (Recovery Time Objectives por sus siglas en inglés RTO).	Control de Simulacros
			Lista de estrategias definidas y probadas
		Punto Objetivo de Recuperación (Recovery Time Objectives por sus siglas en inglés RPO).	Control de recuperación ante desastres: tiempo e impacto económico

Fuente: Elaborado por el Investigador

Variable Dependiente: Disponibilidad de los servicios de TI

Tabla 6. Operacionalización de la Variable Dependiente

Variable	Definición Conceptual	Indicadores	Sub-Indicador
Disponibilidad de los Servicios Críticos de TI	Son aquellos servicios estratégicos y tecnológicos requeridos por las áreas prioritarias del negocio.	Tiempo Necesario para activar los sistemas críticos de TI	Tiempo de movilización o reubicación de equipos. ***** Tiempo de activación del sitio alternativo ***** Total, de Caídas de los sistemas críticos ***** Tiempos de recuperación de los sistemas críticos

Fuente: Elaborado por el Investigador

3.8. Hipótesis

Es necesario asumir ciertas hipótesis las cuales ayudan a especificar los posibles eventos de interrupción y las capacidades de recuperación de la empresa, las relaciones que deben analizarse respecto al impacto positivo según la capacidad de prevención, recuperación e impacto negativo de los eventos se pueden ligar a:

- Si la interrupción ocurre en ocasiones donde el procesamiento es máximo.
- Si no existe facilidad de recuperación alterna de TI.
- Si no existe un área de trabajo u oficina alterna.
- Si no existe facilidad para operar y producir de forma alterna.
- Si el sitio afectado se vuelve inaccesible una vez ocurrida la interrupción.

- Si el sitio afectado se vuelve accesible después de un periodo de tiempo después de ocurrida la interrupción.

3.8.1 Hipótesis de trabajo o de investigación.

La ejecución del plan de continuidad de negocios impacta positivamente en la recuperación, restauración y disponibilidad de los servicios y equipos críticos de TI, en Droguería y Laboratorio Henie Farma S. de R. L.

3.8.2 Hipótesis nula.

La ejecución del plan de continuidad de negocios no impacta positivamente en la recuperación, restauración y disponibilidad de los servicios críticos de TI, en Droguería y Laboratorio Henie Farma S. de R. L.

Capítulo IV. Resultados del Estudio y Análisis de Resultados

4.1 Pretest

Datos relevantes previo a las acciones de pruebas de continuidad: simulacro #1

Instrumento 3.5.2.1 - Evaluación preliminar del plan de continuidad

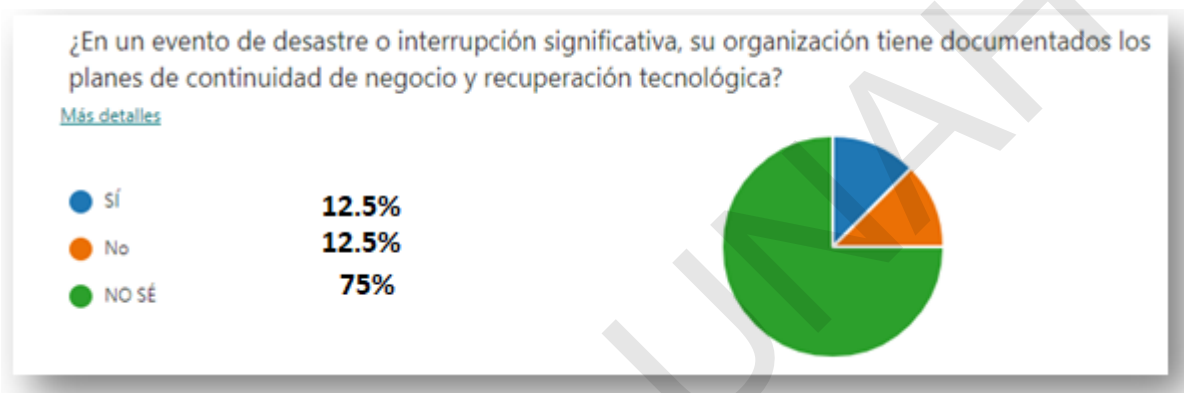


Figura 7. Documentación de los planes de continuidad

Nota. Se muestra desconocimiento general de la existencia o no de planes que dicten las pautas a seguir en casos de interrupciones de los servicios o sistemas críticos de TI.

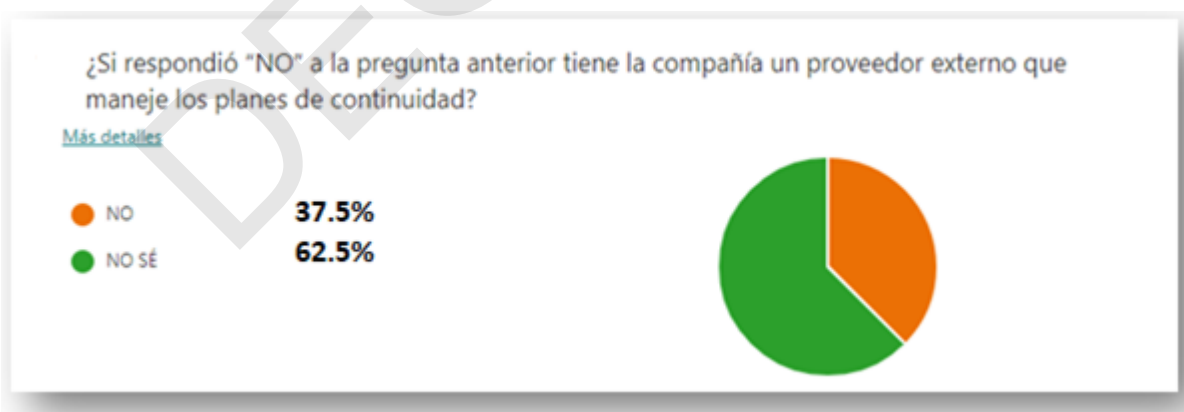


Figura 8. Proveedores externos que apoyen en la continuidad del negocio.

Nota. Los resultados muestran desconocimiento del tema y los que conocen afirman que no existe soporte de terceros.

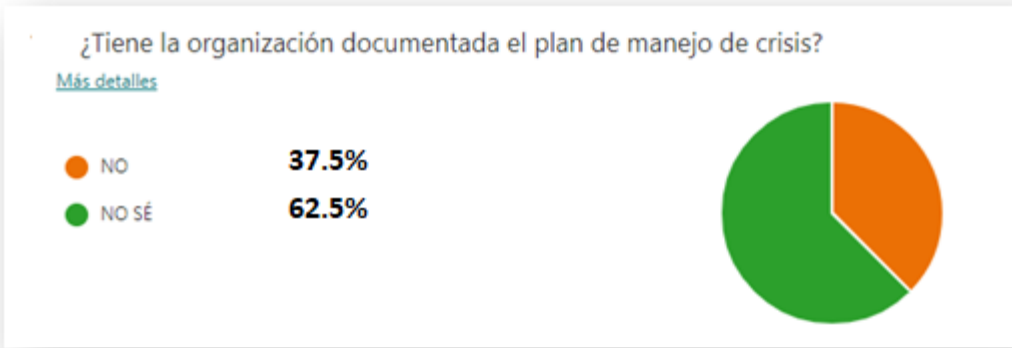


Figura 9. Documentación del plan de manejo de crisis.

Nota: A nivel general se confirma que la empresa no posee un plan de manejo de crisis, el cual es de utilidad al momento de eventos disruptivos, además de formar parte del plan de continuidad.

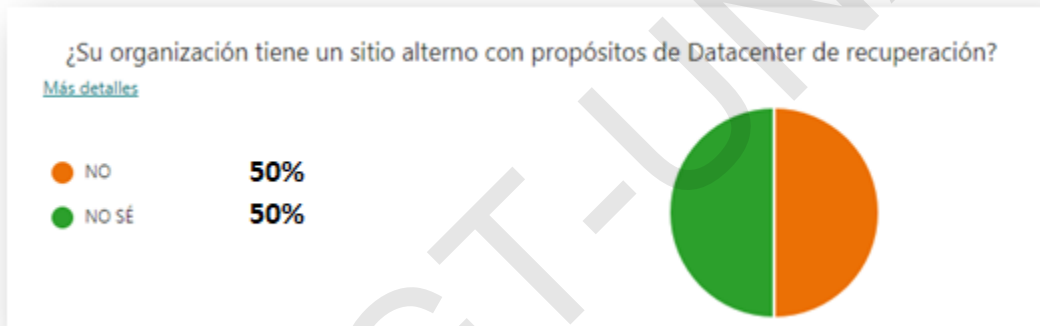


Figura 10. Existencia de Sitio Alternativo.

Nota: Desconocimiento parcial del tema, afirmación parcial de no contar con un sitio alternativo, el cual es fundamental para garantizar la continuidad del negocio en caso de eventos catastróficos.

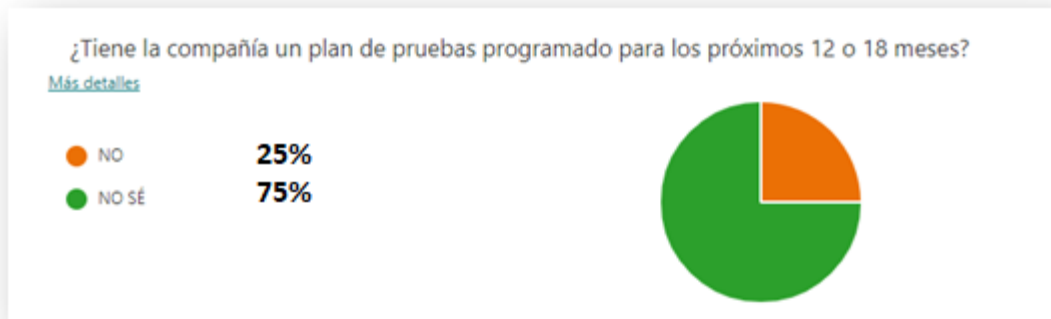


Figura 11. Calendarización de un plan de pruebas.

Nota. El estudio inicial refleja desconocimiento total de la existencia de un plan.

Es evidente el desconocimiento de la existencia o no de un Plan de Continuidad de los Servicios de TI por parte de los usuarios claves de Henie Farma, a pesar de que el área de Tecnología si maneje documentación relacionada, la misma no ha sido formalizada. La falta de formalización de acciones respecto a la Continuidad de los servicios críticos de TI, carencia de recursos como sitio alternativo o programación de pruebas, representan una evidente debilidad respecto a los planes de prevención y recuperación.

Instrumento 3.5.2.3 - Lista De Chequeo De Notificaciones

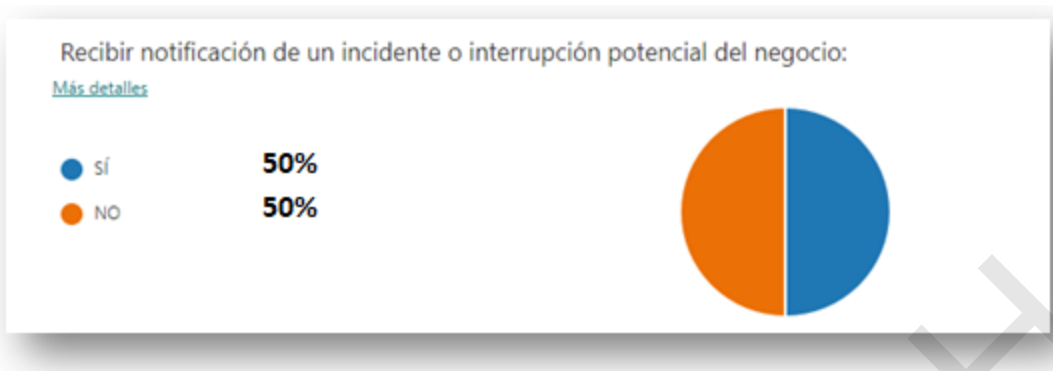


Figura 12. Notificación de incidentes.

Nota. Se refleja parcialmente la no conformidad respecto a los avisos en caso de disrupciones de los servicios o equipos críticos de TI, los cuales afectan la operativa del negocio.

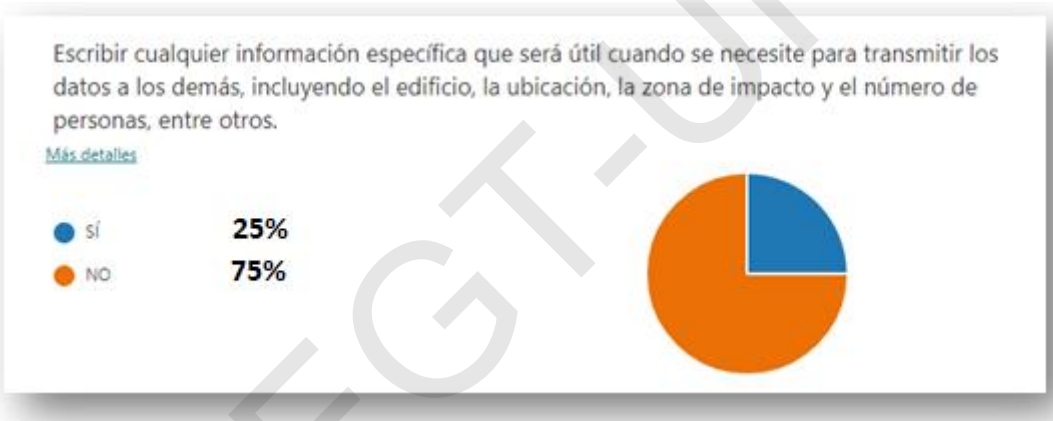


Figura 13. Detalle de Notificaciones.

Nota. Reflejar cualquier dato sobre la disrupción de los equipos o servicios, los cuales serán de utilidad para evaluar la magnitud de daños, estrategias de recuperación, etc. Se reflejan resultados negativos en cuanto a la bitácora informativa.

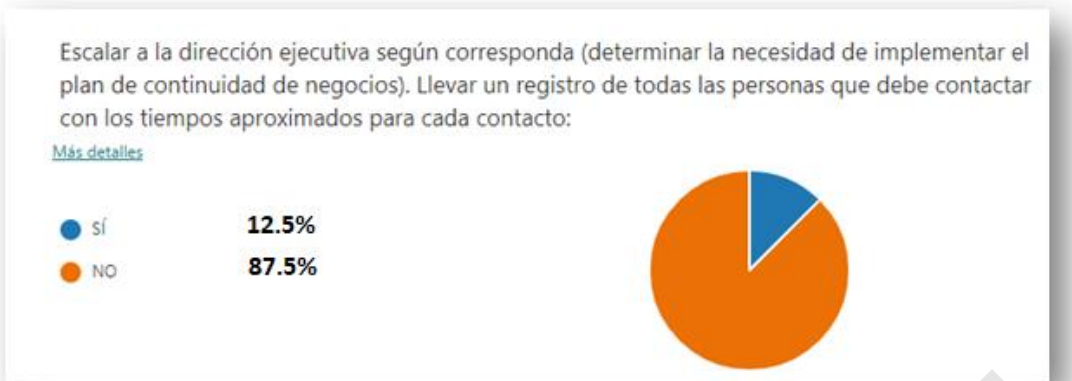


Figura 14. Escalamiento gerencial

Nota. Permite documentar el personal clave para reaccionar a un incidente, activar alarmas de notificación a la alta gerencia con el fin de obtener autorizaciones de la alta gerencia. Se evidencia la falta de notificación y comunicación al personal clave.



Figura 15. Data Center Alterno.

Nota. Menciona la existencia de un sitio de operaciones de TI alternativo, ubicado en un sitio geográfico diferente al principal. Es evidente que no se cuenta con sitio alternativo.

La lista de notificaciones previa al simulacro pretende reflejar cuan informados están los usuarios que conocen y operan bajo los sistemas y equipos críticos de la empresa, a fin de garantizar respuestas óptimas respecto a las acciones de recuperación. Los resultados generales de las pruebas “pretest”, muestran por parte de los usuarios clave de Henie Farma una clara deficiencia en las medidas de respuesta, ya que no poseen una guía que les permita orientar esfuerzos y coordinar acciones.

Instrumento 3.5.2.4 - Lista De Chequeo De Respuesta

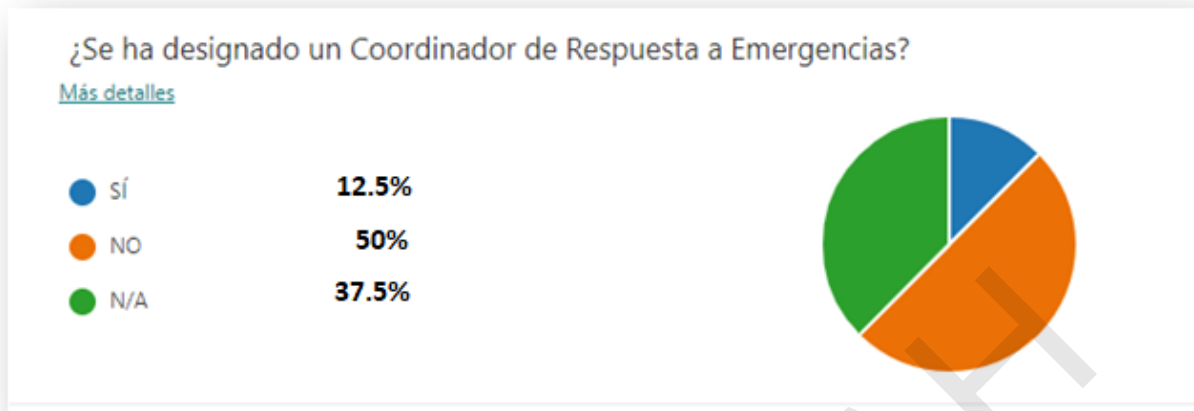


Figura 16. Coordinador de respuesta a emergencias.

Nota. El coordinador de respuesta a emergencias es la persona encargada de activar las alertas a la alta gerencia y personal clave ante eventos disruptivos. Los resultados reflejan incertidumbre en la existencia o no de dicho coordinador.

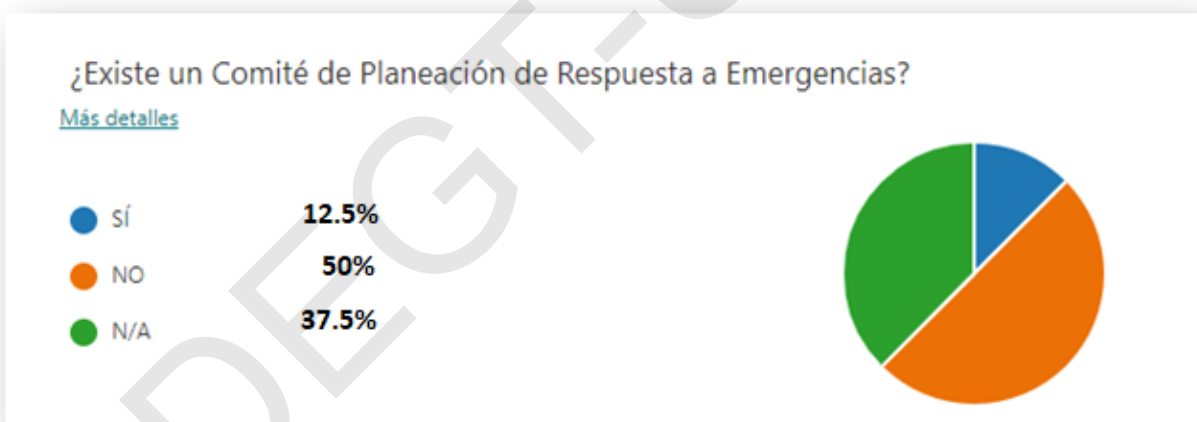


Figura 17. Comité de respuesta a emergencias.

Nota. Los comités de respuesta a emergencias son formados en base a la seguridad ocupacional, tienen la responsabilidad principal de garantizar que se utilicen adecuadamente los recursos disponibles para atender la emergencia, y procurar salvaguardar las vidas y recursos posiblemente afectados. Los datos muestran desconocimiento del tema.

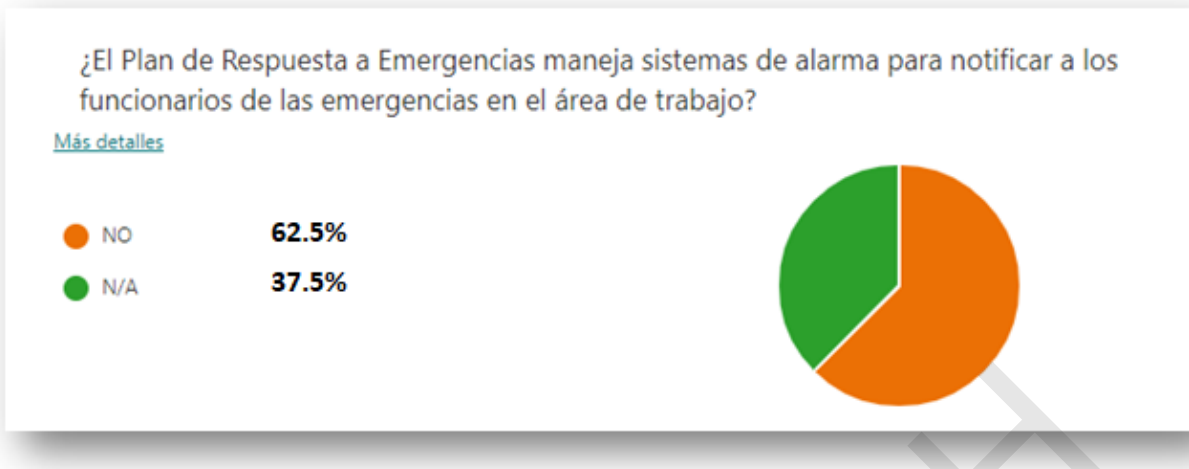


Figura 18. Sistemas de alarma.

Nota. Los sistemas de alarma permiten alertar a las personas de una determinada edificación que se encuentra en riesgo inminente y que deben trasladarse a una zona más segura. Se desconoce la existencia de dichas alarmas de emergencia.

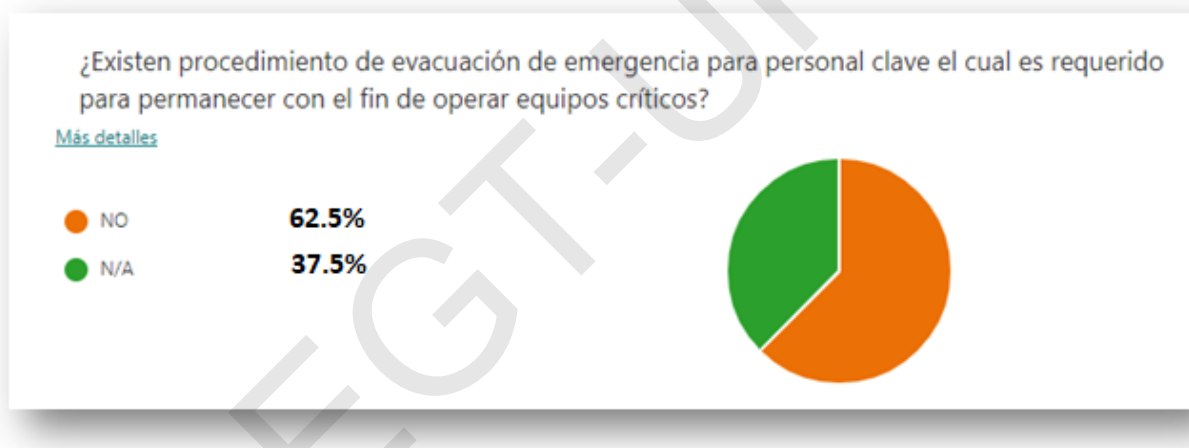


Figura 19. Procedimiento de evacuación para personal clave.

Nota. Respecto a la recuperación de los servicios o equipos críticos ante una emergencia, el personal clave encargado de operar durante una catástrofe debe ser respaldado por planes de evacuación alternos. Los datos siguen reflejando incertidumbre respecto al tema de evacuación de emergencia.

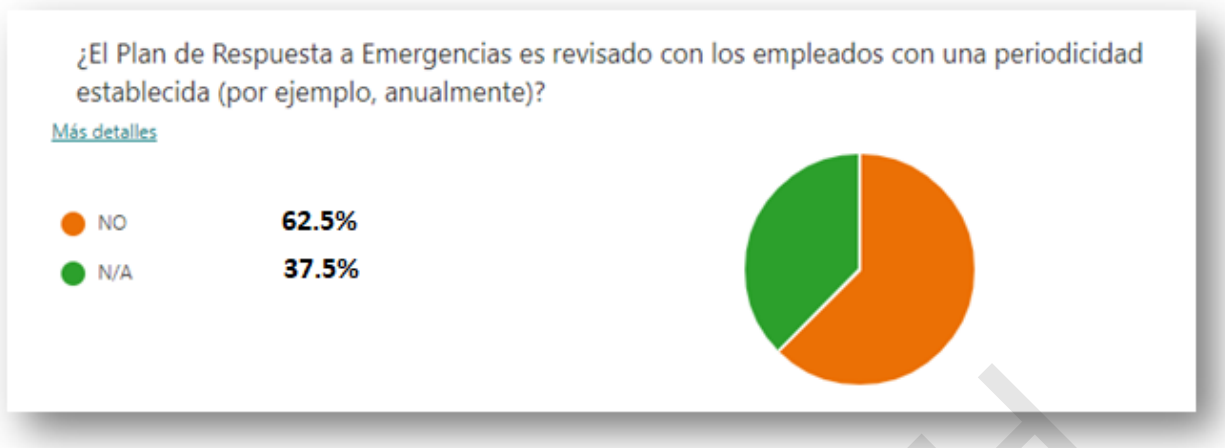


Figura 20. Periodicidad del plan de respuesta a emergencias.

Nota. La revisión permanente de los planes de respuesta a emergencias es fundamental para garantizar el correcto accionar al momento de un incidente. Se refleja falta de socialización del plan.

Las listas de Chequeo de Respuestas darán la pauta de si podrán obtener resultados positivos y productivos en los simulacros, estos resultados se basan en una lista de verificación que ofrezca una probabilidad alta de que el plan de respuesta a emergencias se comportará bien durante el simulacro, la relación con la continuidad de negocios de los servicios y equipos críticos de TI es muy estrecha, los resultados pretest muestran una clara informalidad del conocimiento del proceso de manejo ante emergencias, esto radica en la no integridad del plan de emergencias.

Instrumento 3.5.2.5 - Evaluación de Análisis de Impacto del Negocio (Business

Impact Analysis por sus siglas en inglés BIA)

Simulacro #1. 12/06/2021 – Oficina Henie Farma, Tegucigalpa-Honduras

BIA – Analizando Resultados respecto al Simulacro #1

Tabla 7. BIA: valoración del impacto Financiero.

Financiero	Escala de Impacto: Porcentaje aplicado sobre el presupuesto de Henie Farma para el año 2021: L 25 millones	
Importancia		%
Baja	mayor que 0 - menor o igual que 2.5%	25%
Media	mayor que 2.5% - menor o igual que 6.5%	25%
Alta	mayor que 6.5%	50%

Tabla 8. BIA: valoración del impacto reputacional.

Reputacional	Escala de Impacto	
Descripción		%
Baja	No afecta la buena imagen del Entidad.	12.5%
Media	Mala imagen a nivel de la Industria Farmacéutica.	12.5%
Alta	Mala imagen a nivel Nacional (Clientes)	75%

Tabla 9. BIA: valoración del impacto operacional.

Operacional	Escala de Impacto:	
Descripción		%
Baja	Afecta menos del 25% de las actividades normales de la empresa.	75%
Media	Afecta entre el 25% y el 80% de las actividades normales de la empresa.	25%
Alta	Afecta más del 80% de las actividades normales de la empresa.	0%

Los resultados respecto al BIA reflejan datos un tanto superficiales respecto a las posibles pérdidas que tendría la empresa al detener operaciones por la caída de los servicios de TI, desconocer los tiempos de retorno de los servicios, sistemas o equipos que permiten la comercialización y producción de los productos que la empresa produce y distribuye, son las aristas que lo determinan.

Instrumentos 3.5.2.6 - Plantillas para Registrar la Activación, Recuperación y Restauración del Plan de Continuidad de Negocios – Simulacro #1

Tabla 10. Plantilla de Activación (Sistemas y Servicios): Simulacro

PLANTILLA PLAN DE ACTIVACIÓN (Servicios y Sistemas)								
Actividades críticas	Acciones de Activación	Recursos, requerimientos	RTO/Mins	RTO/Resultado	RPO/Mins	RPO/Resultado	Completado (SI/NO)	Observaciones
Sistemas Aspel (SAE, COI, BAN, PROD, SAE-Móvil, Bases de Datos)	Detener Servicios Aspel: Base de datos y gestor de licencias	Servidor de Virtualización	N/A	N/A	N/A	N/A	SÍ	Se procede a detener los servicios de base de datos y aplicativos ASPEL
Sistemas para Control de Calidad	Desconectar la unidad de red del servidor de aplicativos	Servidor de Aplicativos (virtual)	N/A	N/A	N/A	N/A	SÍ	
Servicios Web (Intranet, Sitio Web, Sistema de Canjes, visita Médica, GLPI, Office 365)	Bloquear credenciales administrador sitio web, Sistema de canjes y visita médica, detener servicio GLPI y bloquear administrador de Office 365	Internet	N/A	N/A	N/A	N/A	SÍ	
PBX	Detener servidor ISSABEL-PBX	Servidor PBX	N/A	N/A	N/A	N/A	SÍ	

PLANTILLA PLAN DE ACTIVACIÓN (Servicios y Sistemas)								
CCTV	Simular cambio disco duro y reinicio de NVR	NVR, Discos Duros de respaldo	N/A	N/A	N/A	N/A	SÍ	
Sistemas Planta de Producción	Mantenimiento de emergencia de equipos, detener software	Equipos para la producción de etiquetas, vaciado de tubos, etc.	N/A	N/A	N/A	N/A	SÍ	
Enlace Internet	Simular caída Internet Tigo: reinicio router y tiempo de respuesta soporte técnico del proveedor	Router del ISP	N/A	N/A	N/A	N/A	SÍ	

Nota. Acciones por realizar en un simulacro respecto a la interrupción de los equipos o servicios, generar la interrupción o caída de estos.

Tabla 11. Plantilla de Activación (Equipos): Simulacro

PLANTILLA PLAN DE ACTIVACIÓN (Equipos)								
Equipos críticos	Acciones de Activación	Recursos, requerimientos	RTO/Mi nutos	RTO/Mi nutos	RPO/Resul tado	RPO/Resul tado	Completado (SI/NO)	Observaciones
Servidor Virtualizado	Detener server, similar fallo de hardware y software	Servidor Virtualizado	N/A	N/A	N/A	N/A	SÍ	
Servidor PBX	Detener server, simular fallo de hardware y software	Servidor PBX	N/A	N/A	N/A	N/A	SÍ	
Servidor de Archivos	Detener server, simular fallo de hardware y software	Servidor de Archivos	N/A	N/A	N/A	N/A	SÍ	
Switches Administrables	Detener equipos, similar fallo de hardware/software	Switches	N/A	N/A	N/A	N/A	SÍ	
Reuters Wireless	Detener equipos, similar fallo de hardware/software	Router's	N/A	N/A	N/A	N/A	SÍ	

Nota. Acciones por realizar en un simulacro respecto a la interrupción de los equipos o servicios, generar la interrupción o caída de estos.

Tabla 12. Plantilla de Recuperación (Servicios y Sistemas): Simulacro

PLANTILLA PLAN DE RECUPERACIÓN (Servicios y Sistemas)								
Actividades críticas	Acciones de Recuperación	Recursos, requerimientos	RTO/Minutos	RTO/Resultado	RPO/Transacciones	RPO/Resultado	Completado (SI/NO)	Observaciones
Sistemas Aspel (SAE, COI, BAN, PROD, SAE-Móvil, Bases de Datos)	Restablecer Servicios Aspel: Base de datos y gestor de licencias	Servidor Virtualizado	20	40	5	10	SÍ	Se procede a detener los servicios de base de datos y aplicativos ASPEL
Sistemas para Control de Calidad	Mapear la unidad de red del servidor de aplicativos	Servidor de Aplicativos (virtual)	10	120	10	50	SÍ	Tiempo y registros en los sistemas
Servicios Web (Intranet, Sitio Web, Sistema de Canjes, visita Médica, GLPI, Office 365)	Desbloquear credenciales administrador sitio web, Sistema de canjes y visita médica, detener servicio GLPI y desbloquear administrador de Office 365	Internet	60	120	50	50	SÍ	Tiempo y Registros en los sistemas

PLANTILLA PLAN DE RECUPERACIÓN (Servicios y Sistemas)								
PBX	Reiniciar servidor, cambio de equipo, migrar ISSABEL-PBX	Servidor PBX	20	180	10	45	SÍ	Tiempo y Llamadas perdidas
CCTV	Simular cambio disco duro y reinicio de NVR	NVR, Discos Duros de respaldo	25	120	10	120	SÍ	Minutos de video
Sistemas Planta de Producción	Reiniciar equipos y software	Equipos para la producción de etiquetas, vaciado de tubos, etc.	30	120	N/A	N/A	SÍ	Tiempo perdido en ordenes de producción
Enlace Internet	Simular caída Internet Tigo: reinicio router y tiempo de respuesta soporte técnico del proveedor	Router del ISP	120	480	N/A	N/A	SÍ	Tiempo restaurar internet por parte del ISP

Nota. Acciones por realizar en un simulacro respecto a la evaluación de alternativas y pruebas para poner en marcha de los equipos o servicios, posterior a una interrupción o caída de estos.

Tabla 13. Plantilla de Recuperación (Equipos): Simulacro

PLANTILLA PLAN DE RECUPERACIÓN (Equipos)								
Equipos críticos	Acciones de Recuperación	Recursos, requerimientos	RTO/Minutos	RTO/Minutos	RPO/Resultado	RPO/Resultado	Completado (SI/NO)	Observaciones
Servidor Virtualizado	Revisión física, reinicio y revisión de Sistema operativo y Hyper V	Servidor Virtualizado	120	2,880	N/A	N/A	SÍ	Simulación sin contemplar equipos y sistemas alternos
Servidor PBX	Revisión física, reinicio y revisión de Sistema operative	Servidor PBX	120	2,880	N/A	N/A	SÍ	Simulación sin contemplar equipos y sistemas alternos
Servidor de Archivos	Revisión física, reinicio y revisión de Sistema operative	Servidor de Archivos	120	2,880	N/A	N/A	SÍ	Simulación sin contemplar equipos y sistemas alternos
Switches Administrables	Revisión física y Reinicio de equipos	Switches	30	360	N/A	N/A	SÍ	Simulación sin contemplar equipos y sistemas alternos
Router's Wireless	Revisión física y Reinicio de equipos	Router's	30	360	N/A	N/A	SÍ	Simulación sin contemplar equipos y sistemas alternos

Nota. Acciones por realizar en un simulacro respecto a la evaluación de alternativas y pruebas para poner en marcha de los equipos o servicios, posterior a una interrupción o caída de estos.

Tabla 14. Plantilla plan de restauración (servicios y sistemas): Simulacro.

PLANTILLA PLAN DE RESTAURACIÓN (Servicios y Sistemas)								
Actividades críticas	Acciones de Restauración	Recursos, requerimientos	RTO/Minutos	RTO/Resultado	RPO/Transacciones	RPO/Resultado	Completado (SI/NO)	Observaciones
Sistemas Aspel (SAE, COI, BAN, PROD, SAE-Móvil, Bases de Datos)	Restablecer sistemas mediante copia de respaldo	Servidor Virtualizado, copias de respaldo	120	300	50	200	SÍ	Sin el uso del plan de backup diario sería considerable la pérdida de datos
Sistemas para Control de Calidad	Mapear la unidad de red del servidor de aplicativos	Servidor de Aplicativos (virtual)	60	300	20	250	SÍ	Sin el uso del plan de backup diario sería considerable la pérdida de datos
Servicios Web (Intranet, Sitio Web, Sistema de Canjes, visita Médica, GLPI, Office 365)	Desbloquear credenciales administrador sitio web, Sistema de canjes y visita médica, detener servicio GLPI y desbloquear administrador de Office 365	Internet	60	240	N/A	N/A	SÍ	Restauración desde copias de respaldo de los equipos y reemplazo de equipos.
PBX	Reiniciar servidor, cambio de equipo,	Servidor PBX	60	180	20	50	SÍ	Restauración desde copias de respaldo de los equipos y reemplazo

PLANTILLA PLAN DE RESTAURACIÓN (Servicios y Sistemas)								
	migrar ISSABEL-PBX							de equipos.
CCTV	Reiniciar, cambio de equipo	NVR, Discos Duros de respaldo	20	240	20	240	SÍ	Datos respecto por no contar con equipos alternos (RPO pérdidas tiempo video grabación)
Sistemas Planta de Producción	Reiniciar equipos y software	Equipos para la producción de etiquetas, vaciado de tubos, etc.	30	480	N/A	N/A	SÍ	Datos respecto por no contar con equipos alternos
Enlace Internet	Simular caída Internet Tigo: reinicio router y tiempo de respuesta soporte técnico del proveedor	Router del ISP	120	480	N/A	N/A	SÍ	Tiempo restaurar internet por parte del ISP

Nota. Acciones por realizar en un simulacro respecto a la puesta en marcha de los equipos o servicios, posterior a una interrupción o caída de estos.

Tabla 15. Plantilla de Restauración (Equipos): Simulacro

PLANTILLA PLAN DE RESTAURACIÓN (Equipos)								
Equipos críticos	Acciones de Restauración	Recursos, requerimientos	RTO/Minutos	RTO/Minutos	RPO/Resultado	RPO/Resultado	Completado (SI/NO)	Observaciones
Servidor Virtualizado	Migrar a servidor alternativo, sitio alternativo o la nube	Servidor Virtualizado	180	4,320	N/A	N/A	SÍ	Simulación sin contemplar equipos y sistemas alternos
Servidor PBX	Migrar a servidor alternativo, sitio alternativo o la nube	Servidor PBX	120	4,320	N/A	N/A	SÍ	Simulación sin contemplar equipos y sistemas alternos
Servidor de Archivos	Migrar a servidor alternativo, sitio alternativo o la nube	Servidor de Archivos	120	4,320	N/A	N/A	SÍ	Simulación sin contemplar equipos y sistemas alternos
Switches Administrables	Migrar a equipos alternativo	Switches	30	1,440	N/A	N/A	SÍ	Simulación sin contemplar equipos y sistemas alternos
Router's Wireless	Migrar a equipos alternativo	Router's	30	1,440	N/A	N/A	SÍ	Simulación sin contemplar equipos y sistemas alternos

Nota. Acciones por realizar en un simulacro respecto a la puesta en marcha de los equipos o servicios, posterior a una interrupción o caída de estos.

Las plantillas de activación, recuperación y restauración reflejan información muy coherente sobre las posibles pérdidas que se pueden tener en la empresa al ocurrir una caída de los servicios críticos de TI, no contar con un plan de continuidad del negocio

respecto a estos constituyen un riesgo latente, todo ello al no poder tener instrucciones formalizadas y socializadas de qué hacer y cómo accionar; por último el riesgo de no tener equipos alternos que puedan garantizar la activación del plan.

Instrumento 3.5.2.8 - Plantilla de Experiencia del usuario y evaluación de los simulacros

Tabla 16. Experiencia de usuario.

VALORACIÓN GENERAL – PROMEDIO	Valor Max 10 – Min 0
Definición clara de los objetivos del simulacro	4
Identificación de los recursos necesarios	3
Participación en el simulacro los usuarios necesarios	7
Disponibilidad de los recursos necesarios para la restauración de los servicios	2
La complejidad del ejercicio fue adecuada para los posibles eventos reales	3
Se reanudaron en tiempo y forma los sistemas y equipos	1
Se identificaron los posibles escenarios de fallos	6
El Plan de continuidad de negocios, mejorará la disponibilidad de los Sistemas de información	1
Correcta comunicación de la planificación de los simulacros	1
Los usuarios claves respondieron de manera adecuada al simulacro.	2
<i>Porcentaje de Valoración General respecto al Simulacro #1 sin conocer el Plan de Continuidad</i>	30%
% de Éxito → 30% -- 3.0 BAJO	
ALTO → 8.5 – 10 MEDIO → 6 – 8.4 BAJA → 0 – 5.9	

Nota. La tabla de experiencia de usuario tiene como objetivo principal evaluar el simulacro desde la perspectiva de los usuarios clave, los detalles ayudarán a futuras mejoras en el proceso de pruebas. Los resultados bastante contundentes, el no contar o desconocer el Plan de Continuidad del Negocio refleja datos de usuario bastante reales.

4.2 Postest

Datos relevantes previo a las acciones de pruebas de continuidad: simulacro #2

Instrumento 3.5.2- Evaluación preliminar del plan de continuidad

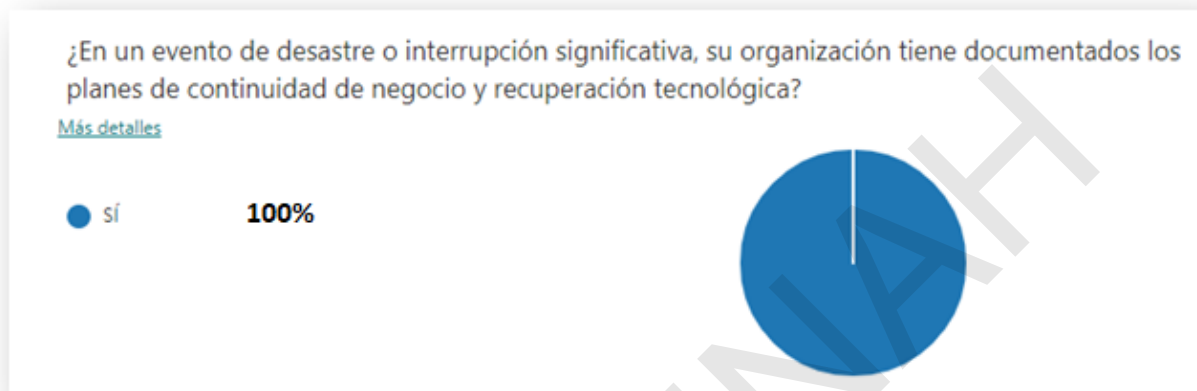


Figura 21. Documentación de los planes de continuidad

Nota. Luego de socializar la documentación de los planes, ya es del conocimiento general la existencia de los estos, por lo que se tienen claridad sobre las pautas a seguir en casos de interrupciones de los servicios o sistemas críticos de TI.

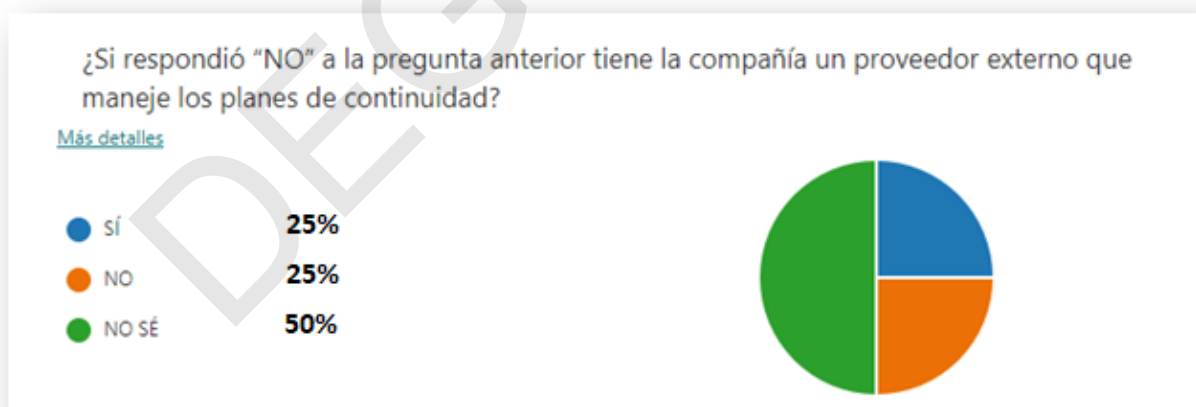


Figura 22. Proveedores externos que apoyen en la continuidad del negocio.

Nota. Los resultados muestran desconocimiento del tema y los que conocen afirman que no existe soporte de terceros, la diferencia posterior al simulacro #1, es que los usuarios clave conocen los proveedores que pueden apoyar de forma parcial ante los eventos de continuidad.

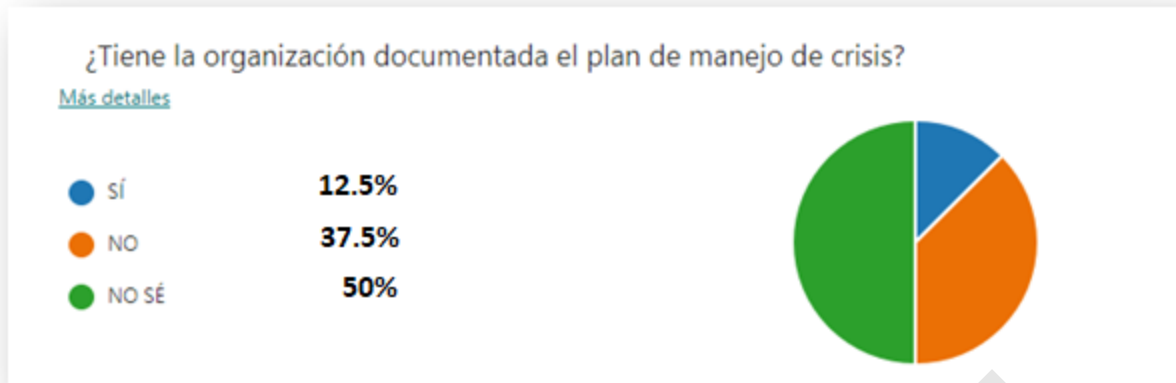


Figura 23. Documentación del plan de manejo de crisis.

Nota: A nivel general se confirma que la empresa no posee o desconoce la existencia de un plan de manejo de crisis, el cual es de utilidad al momento de eventos disruptivos, además de formar parte del plan de continuidad. Se sigue considerando que solo es del conocimiento de la alta gerencia.



Figura 24. Existencia de Sitio Alternativo.

Nota: Desconocimiento parcial del tema, afirmación parcial de no contar con un sitio alternativo, el cual es fundamental para garantizar la continuidad del negocio en caso de eventos catastróficos.

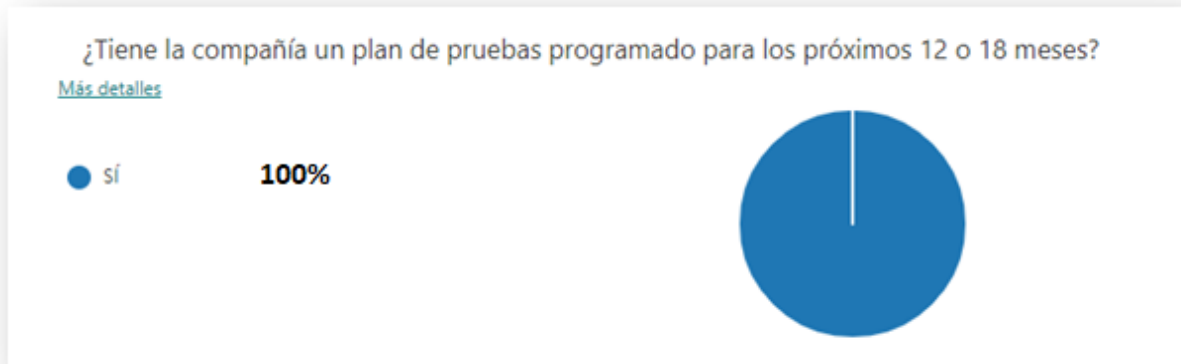


Figura 25. Calendarización de un plan de pruebas.

Nota. El estudio posterior al simulacro #1 refleja la efectiva socialización de la existencia de un plan de pruebas.

Los datos obtenidos previo al Simulacro #2 y posterior al Simulacro #1, reflejan un cambio relevante, al socializar el plan de continuidad del negocio de los sistemas críticos de TI, los usuarios claves obtuvieron la información necesaria para conocer las acciones a seguir en caso de fallos en los sistemas críticos, conocer los tiempos y las personas claves a quien infirmar fueron 2 de los más importantes temas con mayor relevancia.

Instrumento 3.5.2.3 - Lista De Chequeo De Notificaciones

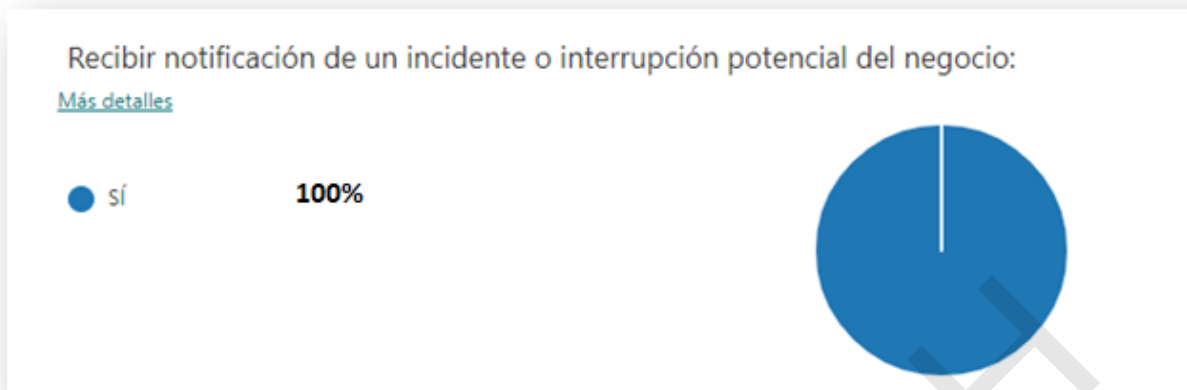


Figura 26. Notificación de incidentes.

Nota. Se refleja parcialmente la total conformidad respecto a los avisos en caso de disrupciones de los servicios o equipos críticos de TI, esto ayudaría a estar preparados previo, durante y después de los fallos.

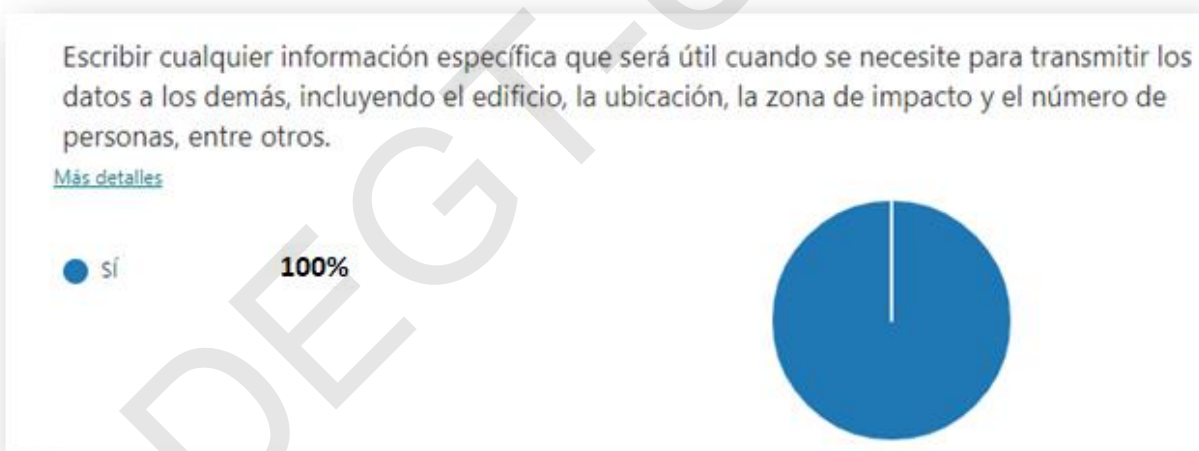


Figura 27. Detalle de Notificaciones.

Nota. Reflejar cualquier dato sobre la disrupción de los equipos o servicios, los cuales serán de utilidad para evaluar la magnitud de daños, estrategias de recuperación, etc. Se reflejan resultados positivos en cuanto a la bitácora informativa, todo esto posterior al simulacro #1.

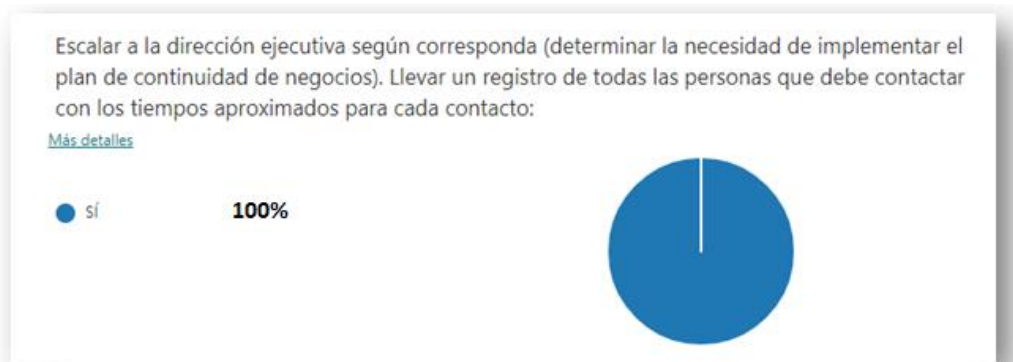


Figura 28. Escalamiento gerencial

Nota. Permite documentar el personal clave para reaccionar a un incidente, activar alarmas de notificación a la alta gerencia con el fin de obtener autorizaciones de la alta gerencia. Se evidencia mejoras en la comunicación de notificaciones al personal clave.

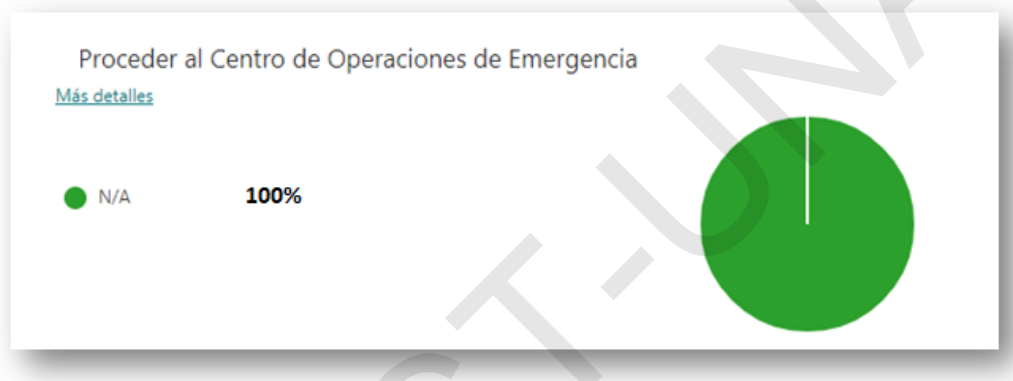


Figura 29. Data Center Alterno.

Nota. Menciona la existencia de un sitio de operaciones de TI alternativo, ubicado en un sitio geográfico diferente al principal. Es evidente que no se cuenta con sitio alternativo.

La lista de notificaciones previa al simulacro pretende reflejar cuan informados están los usuarios que conocen y operan bajo los sistemas y equipos críticos de la empresa, a fin de garantizar respuestas óptimas respecto a las acciones de recuperación. Los resultados generales de las pruebas “postest”, arrojan una clara tendencia de mejora respecto al conocimiento de las acciones que se esperan del personal clave y sobre el papel que cada uno juega en el desarrollo del plan.

Instrumento 3.5.2.4 - Lista De Chequeo De Respuesta

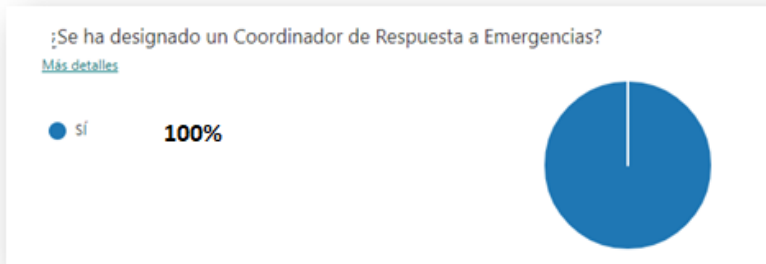


Figura 30. Coordinador de respuesta a emergencias.

Nota. El coordinador de respuesta a emergencias es la persona encargada de activar las alertas a la alta gerencia y personal clave ante eventos disruptivos. Los resultados reflejan conocimiento total de quien es el coordinador.

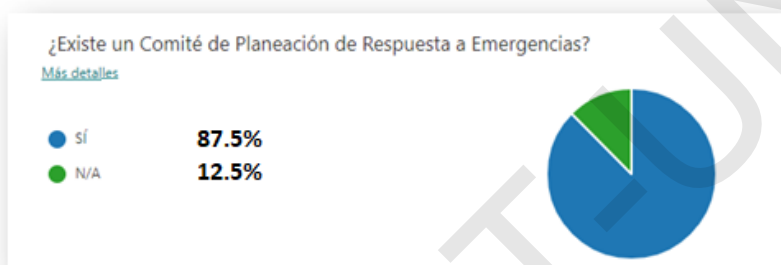


Figura 31. Comité de respuesta a emergencias.

Nota. Los comités de respuesta a emergencias son formados en base a la seguridad ocupacional, tienen la responsabilidad principal de garantizar que se utilicen adecuadamente los recursos disponibles para atender la emergencia, y procurar salvaguardar las vidas y recursos posiblemente afectados. Los datos muestran conocimiento del tema, con posibilidades de mejora.

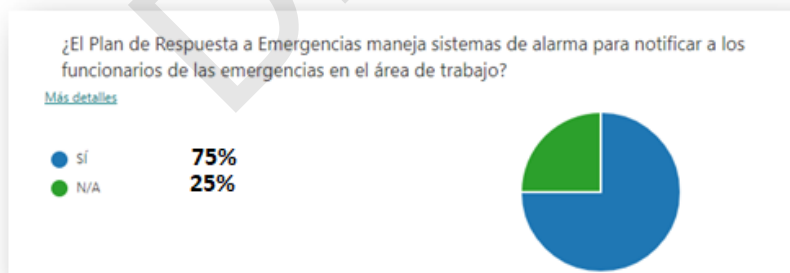


Figura 32. Sistemas de alarma.

Nota. Los sistemas de alarma permiten alertar a las personas de una determinada edificación que se encuentra en riesgo inminente y que deben trasladarse a una zona más segura. Se socializó la existencia de alarmas de emergencia.

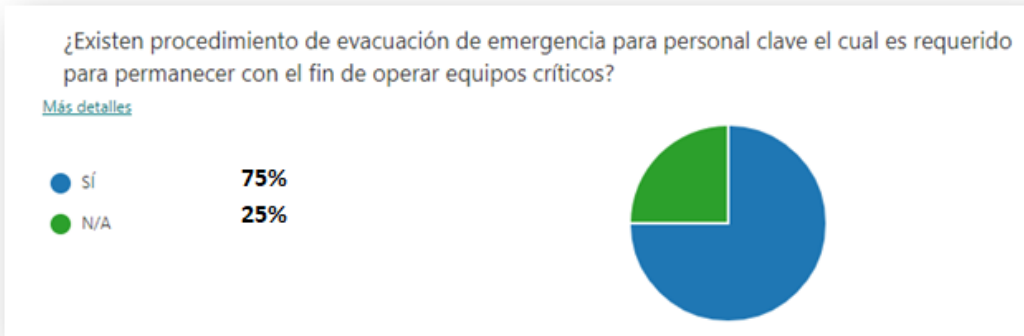


Figura 33. Procedimiento de evacuación para personal clave.

Nota. Respecto a la recuperación de los servicios o equipos críticos ante una emergencia, el personal clave encargado de operar durante una catástrofe debe ser respaldado por planes de evacuación alternos. Los datos reflejan una importante mejora de formalización respecto al tema de evacuación de emergencia.



Figura 34. Periodicidad del plan de respuesta a emergencias.

Nota. La revisión permanente de los planes de respuesta a emergencias es fundamental para garantizar el correcto accionar al momento de un incidente. Se refleja mejoría en la socialización del plan.

Las listas de Chequeo de Respuestas darán la pauta de si se podrán obtener resultados positivos y productivos en los simulacros, estos resultados se basan en una lista de verificación que ofrezca una probabilidad alta de que el plan de respuesta a emergencias se comportará bien durante el simulacro, la relación con la continuidad de negocios de los servicios y equipos críticos de TI es muy estrecha, los resultados pretest muestran una clara informalidad del conocimiento del proceso de manejo ante emergencias, esto radica en la no integridad del plan de emergencias.

Instrumento 3.5.2.5 - Evaluación de Análisis de Impacto del Negocio (Business

Impacto Analysis por sus siglas en inglés **BIA**)

Simulacro #2. 03/07/2021 – Oficina Henie Farma, Tegucigalpa-Honduras

BIA – Analizando Resultados respecto al Simulacro #2

Tabla 17. BIA: Valoración del Impacto Financiero

Financiero	Escala de Impacto: Porcentaje aplicado sobre el presupuesto de Henie Farma para el año 2021: L 25 millones	
Importancia		%
Baja	mayor que 0 - menor o igual que 2.5%	75%
Media	mayor que 2.5% - menor o igual que 6.5%	25%
Alta	mayor que 6.5%	0%

Tabla 18. BIA: Valoración del Impacto reputacional

Reputacional	Escala de Impacto	
Descripción		%
Baja	No afecta la buena imagen del Entidad.	100%
Media	Mala imagen a nivel de la Industria Farmacéutica.	0%
Alta	Mala imagen a nivel Nacional (Clientes)	0%

Tabla 19. BIA: Valoración del Impacto operacional

Operacional	Escala de Impacto:	
Descripción		%
Baja	Afecta menos del 25% de las actividades normales de la empresa.	100%
Media	Afecta entre el 25% y el 80% de las actividades normales de la empresa.	0%
Alta	Afecta más del 80% de las actividades normales de la empresa.	0%

Los resultados que reflejas los valores de impacto del BIA, al ser reconsiderados se puede observar que los usuarios pudieron comprender el impacto real que puede afectar a la empresa, al no contar con planes de recuperación y restauración de los servicios críticos de TI.

Instrumentos 3.5.2.6 - Plantillas para Registrar la Activación, Recuperación y Restauración del Plan de Continuidad de Negocios – Simulacro #2

Tabla 20. Plantilla de Activación (Sistemas y Servicios): Simulacro

PLANTILLA PLAN DE ACTIVACIÓN (Servicios y Sistemas)								
Actividades críticas	Acciones de Activación	Recursos, requerimientos	RTO/Minutos	RTO/Resultado	RPO/Minutos	RPO/Resultado	Completado (SI/NO)	Observaciones
Sistemas Aspel (SAE, COI, BAN, PROD, SAE-Móvil, Bases de Datos)	Detener Servicios Aspel: Base de datos y gestor de licencias	Servidor Virtualizado	N/A	N/A	N/A	N/A	SÍ	Se procede a detener los servicios de base de datos y aplicativos ASPEL
Sistemas para Control de Calidad	Desconectar la unidad de red del servidor de aplicativos	Servidor de Aplicativos (virtual)	N/A	N/A	N/A	N/A	SÍ	
Servicios Web (Intranet, Sitio Web, Sistema de Canjes, visita Médica, GLPI, Office 365)	Bloquear credenciales administrador sitio web, Sistema de canjes y visita médica, detener servicio GLPI y bloquear administrador de Office 365	Internet	N/A	N/A	N/A	N/A	SÍ	

PLANTILLA PLAN DE ACTIVACIÓN (Servicios y Sistemas)								
PBX	Detener servidor ISSABEL-PBX	Servidor PBX	N/A	N/A	N/A	N/A	SÍ	
CCTV	Simular cambio disco duro y reinicio de NVR	NVR, Discos Duros de respaldo	N/A	N/A	N/A	N/A	SÍ	
Sistemas Planta de Producción	Mantenimiento de emergencia de equipos, detener software	Equipos para la producción de etiquetas, vaciado de tubos, etc.	N/A	N/A	N/A	N/A	SÍ	
Enlace Internet	Simular caída Internet Tigo: reinicio router y tiempo de respuesta soporte técnico del proveedor	Router del ISP	N/A	N/A	N/A	N/A	SÍ	

Nota. Acciones por realizar en un simulacro respecto a la interrupción de los equipos o servicios, generar la interrupción o caída de estos.

Tabla 21. Plantilla de Activación (Equipos): Simulacro

PLANTILLA PLAN DE ACTIVACIÓN (Equipos)								
Equipos críticos	Acciones de Activación	Recursos, requerimientos	RTO/Mi nutos	RTO/Mi nutos	RPO/Resul tado	RPO/Resul tado	Completa do(SI/NO)	Observaciones
Servidor Virtualizado	Detener server, simular fallo de hardware y software	Servidor Virtualizado	N/A	N/A	N/A	N/A	SÍ	
Servidor PBX	Detener server, simular fallo de hardware y software	Servidor PBX	N/A	N/A	N/A	N/A	SÍ	
Servidor de Archivos	Detener server, simular fallo de hardware y software	Servidor de Archivos	N/A	N/A	N/A	N/A	SÍ	
Switches Administrables	Detener equipos, simular fallo de hardware/software	Switches	N/A	N/A	N/A	N/A	SÍ	
Router's Wireless	Detener equipos, simular fallo de hardware/software	Router's	N/A	N/A	N/A	N/A	SÍ	

Nota. Acciones por realizar en un simulacro respecto a la interrupción de los equipos o servicios, generar la interrupción o caída de estos.

Tabla 22. Plantilla de Recuperación (Servicios y Sistemas): Simulacro

PLANTILLA PLAN DE RECUPERACIÓN (Servicios y Sistemas)								
Actividades críticas	Acciones de Recuperación	Recursos, requerimientos	RTO/Minutos	RTO/Resultado	RPO/Transacciones	RPO/Resultado	Completado (SI/NO)	Observaciones
Sistemas Aspel (SAE, COI, BAN, PROD, SAE-Móvil, Bases de Datos)	Restablecer Servicios Aspel: Base de datos y gestor de licencias	Servidor Virtualizado	20	30	5	8	SÍ	Tiempos en base al Plan de Continuidad Activo: contemplando equipos alternos y mejores prácticas
Sistemas para Control de Calidad	Mapear la unidad de red del servidor de aplicativos	Servidor de Aplicativos (virtual)	10	15	10	12	SÍ	
Servicios Web (Intranet, Sitio Web, Sistema de Canjes, visita Médica, GLPI, Office 365)	Desbloquear credenciales administrador sitio web, Sistema de canjes y visita médica, detener servicio GLPI y desbloquear administrador de Office 365	Internet	60	60	50	50	SÍ	
PBX	Reiniciar servidor, cambio de equipo, migrar	Servidor PBX	20	20	10	10	SÍ	

PLANTILLA PLAN DE RECUPERACIÓN (Servicios y Sistemas)							
	ISSABEL-PBX						
CCTV	Simular cambio disco duro y reinicio de NVR	NVR, Discos Duros de respaldo	25	30	10	15	SÍ
Sistemas Planta de Producción	Reiniciar equipos y software	Equipos para la producción de etiquetas, vaciado de tubos, etc.	30	30	N/A	N/A	SÍ
Enlace Internet	Simular caída Internet Tigo: reinicio router y tiempo de respuesta soporte técnico del proveedor	Router del ISP	120	60	N/A	N/A	SÍ

Nota. Acciones por realizar en un simulacro respecto a la evaluación de alternativas y pruebas para poner en marcha de los equipos o servicios, posterior a una interrupción o caída de estos.

Tabla 23. Plantilla de Recuperación (Equipos): Simulacro

PLANTILLA PLAN DE RECUPERACIÓN (Equipos)								
Equipos críticos	Acciones de Recuperación	Recursos, requerimientos	RTO/Minutos	RTO/Minutos	RPO/Resultado	RPO/Resultado	Completado (SI/NO)	Observaciones
Servidor Virtualizado	Revisión física, reinicio y revisión de Sistema operativo y Hyper V	Servidor Virtualizado	120	180	N/A	N/A	SÍ	Tiempos en base al Plan de Continuidad Activo: contemplando equipos alternos y mejores prácticas
Servidor PBX	Revisión física, reinicio y revisión de Sistema operative	Servidor PBX	120	180	N/A	N/A	SÍ	
Servidor de Archivos	Revisión física, reinicio y revisión de Sistema operative	Servidor de Archivos	120	180	N/A	N/A	SÍ	
Switches Administrables	Revisión física y Reinicio de equipos	Switches	30	30	N/A	N/A	SÍ	
Router's Wireless	Revisión física y Reinicio de equipos	Router's	30	30	N/A	N/A	SÍ	

Nota. Acciones por realizar en un simulacro respecto a la evaluación de alternativas y pruebas para poner en marcha de los equipos o servicios, posterior a una interrupción o caída de estos.

Tabla 24. Plantilla de Restauración (Servicios y Sistemas): Simulacro

PLANTILLA PLAN DE RESTAURACIÓN (Servicios y Sistemas)								
Actividades críticas	Acciones de Restauración	Recursos, requerimientos	RTO/Minutos	RTO/Resultado	RPO/Transacciones	RPO/Resultado	Completado (SI/NO)	Observaciones
Sistemas Aspel (SAE, COI, BAN, PROD, SAE-Móvil, Bases de Datos)	Restablecer sistemas mediante copia de respaldo	Servidor Virtualizado, copias de respaldo	120	180	50	80	SÍ	Tiempos en base al Plan de Continuidad Activo: contemplando equipos alternos y mejores prácticas
Sistemas para Control de Calidad	Mapear la unidad de red del servidor de aplicativos	Servidor de Aplicativos (virtual)	60	60	20	25	SÍ	
Servicios Web (Intranet, Sitio Web, Sistema de Canjes, visita Médica, GLPI, Office 365)	Desbloquear credenciales administrador sitio web, Sistema de canjes y visita médica, detener servicio GLPI y desbloquear administrador de Office 365	Internet	60	60	N/A	N/A	SÍ	

PLANTILLA PLAN DE RESTAURACIÓN (Servicios y Sistemas)							
PBX	Reiniciar servidor, cambio de equipo, migrar ISSABEL-PBX	Servidor PBX	60	60	20	20	SÍ
CCTV	Reiniciar, cambio de equipo	NVR, Discos Duros de respaldo	20	25	20	20	SÍ
Sistemas Planta de Producción	Reiniciar equipos y software	Equipos para la producción de etiquetas, vaciado de tubos, etc.	30	35	N/A	N/A	SÍ
Enlace Internet	Simular caída Internet Tigo: reinicio router y tiempo de respuesta soporte técnico del proveedor	Router del ISP	120	180	N/A	N/A	SÍ

Nota. Acciones por realizar en un simulacro respecto a la puesta en marcha de los equipos o servicios, posterior a una interrupción o caída de estos.

Tabla 25. Plantilla de Restauración (Equipos): Simulacro

PLANTILLA PLAN DE RESTAURACIÓN (Equipos)								
Equipos críticos	Acciones de Restauración	Recursos, requerimientos	RTO/Minutos	RTO/Minutos	RPO/Resultado	RPO/Resultado	Completado (SI/NO)	Observaciones
Servidor Virtualizado	Migrar a servidor alternativo, sitio alternativo o la nube	Servidor Virtualizado	180	240	N/A	N/A	SÍ	Simulación Contemplando equipos y sistemas alternos
Servidor PBX	Migrar a servidor alternativo, sitio alternativo o la nube	Servidor PBX	120	180	N/A	N/A	SÍ	
Servidor de Archivos	Migrar a servidor alternativo, sitio alternativo o la nube	Servidor de Archivos	120	180	N/A	N/A	SÍ	
Switches Administrables	Migrar a equipos alternos	Switches	30	60	N/A	N/A	SÍ	
Router's Wireless	Migrar a equipos alternos	Router's	30	60	N/A	N/A	SÍ	

Nota. Acciones por realizar en un simulacro respecto a la puesta en marcha de los equipos o servicios, posterior a una interrupción o caída de estos. Las plantillas de restauración y recuperación reflejan datos muy positivos, los tiempos de tolerancia y la cantidad de data que se pueda perder, se encuentran dentro de los rangos tolerables, todo esto responde a la existencia del plan de continuidad y a poseer equipos alternos que garanticen la disponibilidad de los servicios críticos de TI.

Instrumento 3.5.2.8 Plantilla de Experiencia del usuario y evaluación de los simulacros**Tabla 26.** Experiencia de usuario.

VALORACIÓN GENERAL – PROMEDIO	Valor Max 10 – Min 0
Definición clara de los objetivos del simulacro	10
Identificación de los recursos necesarios	9
Participación en el simulacro los usuarios necesarios	10
Disponibilidad de los recursos necesarios para la restauración de los servicios	9
La complejidad del ejercicio fue adecuada para los posibles eventos reales	9
Se reanudaron en tiempo y forma los sistemas y equipos	10
Se identificaron los posibles escenarios de fallos	10
El Plan de continuidad de negocios, mejorará la disponibilidad de los Sistemas de información	10
Correcta comunicación de la planificación de los simulacros	9
Los usuarios claves respondieron de manera adecuada al simulacro.	9
<i>Porcentaje de Valoración General respecto al Simulacro #2 sin conocer el Plan de Continuidad</i>	95%
% de Éxito → 95% -- 9.5 ALTO	
ALTO → 8.5 – 10 MEDIO → 6 – 8.4 BAJO → 0 – 5.9	

Nota. Los usuarios claves posterior al Simulacro #2, reflejan un conocimiento claro respecto a los simulacros y las acciones a seguir respecto a las caídas de los servicios críticos de TI. De esta manera resulta positivo la implementación del plan de continuidad, una guía clara de las acciones a seguir ante los incidentes de TI se ve reflejado en la valoración de la experiencia del usuario.

4.3 Comparativo: Simulacro #1 (Pre-Test) VRS Simulacro #2 (Post-Test)

Es importante mencionar que los datos recolectados respecto al Simulacro #1 responden al entorno de acciones realizadas, sin conocer el plan de continuidad de negocio para Henie Farma; ítems como las valoraciones del impacto económico, reputacional y operativo, las acciones de respuesta y los posibles riesgos que existen en la empresa debido al no tener establecido dicho plan, son el origen de dichos resultados.

Los resultados de la comparativa obedecen a la posible efectividad que tendría la implementación de un plan de continuidad del negocio en Henie Farma S. de R.L., se representarán los ítems más relevantes.

Tabla 27. Comparativo: Simulacro #1 (Pre-Test) VRS Simulacro #2 (Post-Test)

ÍTEMS	S.#1 - % Efectividad/ Valoración	S. #2 - % Efectividad/ Valoración	Observación
Evaluación Preliminar del Plan de Continuidad del Negocio	2.5 %	42 %	Los porcentajes representan el grado de conocimiento del Plan de Continuidad antes de los Simulacros.

ÍTEMS	S.#1 - % Efectividad/ Valoración	S. #2 - % Efectividad/ Valoración	Observación
Lista de Notificaciones	22 %	75 %	Previo a los Simulacros es de suma importancia conocer y evaluar los medios y recursos para activar el Plan de Continuidad, estos porcentajes reflejan el grado de efectividad previo a ambos simulacros.
Lista de Chequeo para Respuestas	4 %	87 %	Grado de efectividad de las acciones de respuesta a una emergencia.
Valoración del Impacto (BIA) – Económico	Alto → 50%	Bajo → 10%	Porcentaje de posible pérdida económica respecto a las ventas mensuales.

ÍTEMS	S.#1 - % Efectividad/ Valoración	S. #2 - % Efectividad/ Valoración	Observación
Valoración del Impacto (BIA) – Operativo	Alto → 75%	Bajo → 15%	Resultados porcentuales respecto a la detención de operaciones.
Valoración del Impacto (BIA) – Reputacional	Medio	Bajo	Respecto a la no atención de los clientes por la falta de los servicios de TI.
RTO/RPO Sistemas y equipos Críticos (Simulacros)	Recuperación → 30 % Restauración → 18 %	Recuperación → 83 % Restauración → 81 %	Porcentajes de eficacia al momento de Recuperar o Restaurar los sistemas y equipos críticos de TI.
Experiencia del Usuario (Simulacros)	30 %	95 %	Valoración de los usuarios clave, respecto a la realización de los Simulacros.

4.4 Análisis de resultados a la luz de la hipótesis

Lo presentado previamente muestra el detalle y análisis de la efectividad del plan de continuidad respecto a los simulacros en sus etapas “Pretest” y “Postest”, en este apartado se presenta la correlación de los resultados con las variables de la investigación y se comprueba la hipótesis con la herramienta MiniTab.

Minitab es una herramienta de análisis de datos potente y de gran reputación con una interfaz intuitiva y fácil de usar tanto para usuarios nuevos como experimentados. Minitab le permite tomar mejores decisiones basadas en datos, al alcance de su mano. (UCESI, 2020)

- **Variable Independiente:** Ejecución del Plan de Continuidad del Negocio
- **Variable Dependiente:** Disponibilidad de los servicios Críticos de TI

Hipótesis

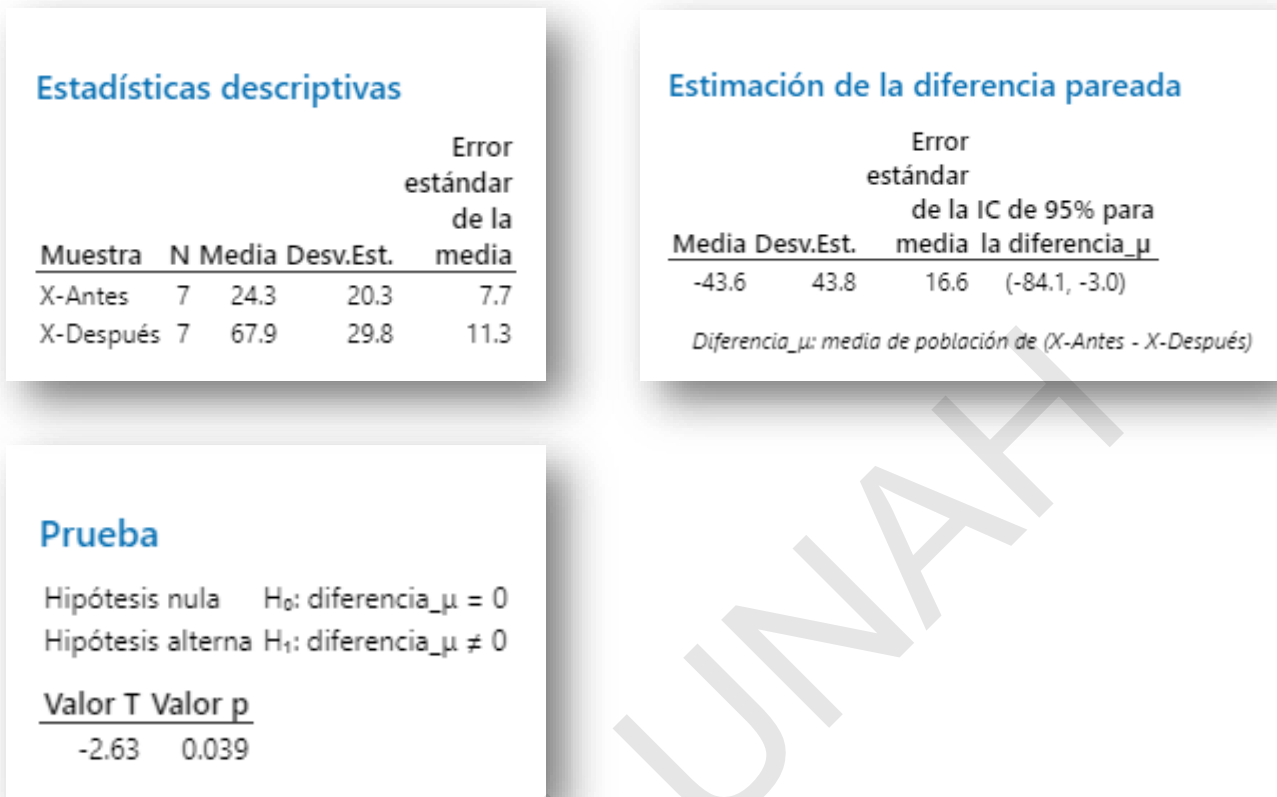
Según los resultados obtenidos de los instrumentos de investigación (más relevantes), se realiza la prueba de la hipótesis con base a los resultados obtenidos: “La ejecución del plan de continuidad de negocios impacta positivamente en la recuperación, restauración y disponibilidad de los servicios y equipos críticos de TI, en Droguería y Laboratorio Henie Farma S. de R. L.”, en la siguiente tabla se muestran los valores para la variable que se llamará X1 (Ejecución del Plan de Continuidad del Negocio, impacto positivo y eficiencia en los tiempos de recuperación y restauración de los servicios críticos de TI) todo esto respecto a los Simulacros #1 antes y Simulacro #2 después.

Tabla 28. Valores porcentuales de la eficacia de la ejecución del plan de continuidad de negocio, para Henie Farma, año 2021.

ÍTEM	X ANTES – Simulacro #1	X DESPUÉS – Simulacro #2
Evaluación Preliminar del Plan de Continuidad del Negocio	3	42
Lista de Notificaciones	22	75
Lista de Chequeo para Respuestas	4	87
Valoración del Impacto (BIA) – Económico	63	12
RTO/RPO Sistemas y equipos Críticos (Simulacros) -- Recuperación	30	83
RTO/RPO Sistemas y equipos Críticos (Simulacros) – Restauración	18	81
Experiencia del Usuario (Simulacros)	30	95

Con los valores para las variables se ingresaron en minitab v20.3 y se procedió a realizar una prueba de tipo “t de student”, la que es recomendada para muestras menores o iguales a 30, este tipo de prueba brinda un tipo de estadística deductiva que se utiliza para determinar si hay una diferencia significativa entre las medias de dos grupos. Con toda la estadística deductiva, se asume que las variables dependientes tienen una distribución normal. Se especifica el nivel de la probabilidad (nivel de la alfa, nivel de la significación, p) que se está dispuesto a aceptar ($p < .05$ es un valor común que se utiliza), lo cual se muestra en la siguiente figura.

Figura 35. Resultado “t de student” con minitab v20.3 para variable X.



Se utilizó la prueba t pareada para analizar el mismo conjunto de elementos que se midieron bajo dos condiciones diferentes, una de ellas respecto al Simulacro #1 y la otra con la experiencia previa de este, durante el Simulacro #2, las diferencias en las mediciones realizadas en la misma variable antes y después reflejan datos contundentes.

Los resultados arrojaron un valor de $T = -2.63$ esto se traduce en $p=0.039$ y como $p < 0.05$ se concluye con que hay suficiente evidencia estadística para aceptar la hipótesis por lo tanto “La ejecución del plan de continuidad de negocios impacta positivamente en la recuperación, restauración y disponibilidad de los servicios y equipos críticos de TI, en Droguería y Laboratorio Henie Farma S. de R. L.”, por lo tanto, la hipótesis es aceptada.

Capítulo V. Conclusiones

- El poder identificar los sistemas, servicios y equipos críticos de TI resulta fundamental para la eficaz implementación de un plan de continuidad, durante esta investigación se encontraron como principales problemas de recuperación de la continuidad operativa de los servicios y equipos críticos de TI, el no contar con redundancia en los mismos, no poseer un sitio alternativo y no contar con los lineamientos formales de cómo actuar en los eventos de caída de los servicios o equipos, lo cual refleja poca inversión tecnológica para robustecer el tema de continuidad operativa de los servicios de TI; de tal manera se puede asegurar que los riesgos y el impacto negativo en las operaciones es alto.
- El aporte profesional del trabajo de investigación presentado es muy valioso para la empresa objeto de estudio, determinar el impacto que el plan de continuidad de negocio tendría en esta, considerando que en la actualidad la empresa no está preparada para afrontar interrupciones o caídas de los servicios y equipos de TI por tiempos prolongados, esto representa un claro análisis para la toma de decisiones de inversión en infraestructura tecnológica; adoptar este tipo de propuestas será el futuro de muchas empresas que apuestan al crecimiento y evolución.
- Posterior a las Pruebas realizadas del plan de continuidad en los simulacros #1 y #2 y los resultados obtenidos mediante los instrumentos de investigación aplicados a los usuarios Clave de Henie Farma, se puede concluir que, al no contar con un plan de continuidad de negocio respecto a los servicios críticos de TI, se ve afectada la disponibilidad de los sistemas de información y equipos críticos de TI; se establecen de igual forma cuales deben

ser los tiempos aceptables de recuperación de dichos sistemas y equipos, los cuales no deben representar un impacto alto en la operativa del negocio.

- Los datos estadísticos obtenidos de las pruebas o simulacros, frente a posibles caídas de los equipos y sistemas críticos, recomiendan definir las políticas de continuidad del negocio, adoptando el Plan sugerido en este estudio de investigación; quedó en evidencia que no se cuenta con una estrategia precisa con tareas y responsables, que ayuden a recuperar el normal funcionamiento de los sistemas y equipos críticos de TI.

Capítulo VI. Aplicabilidad

6.1 Nombre de la Propuesta

Implementación y evaluación de un plan de continuidad del negocio de los servicios de TI, en laboratorio Henie Farma s. De R.L., en Tegucigalpa, año 2021.

6.2 Introducción

Actualmente la importancia de la disponibilidad, integridad y accesibilidad de la información resulta prioritaria para las empresas, poder establecer planes de contingencia que permita manejar, de la mejor forma, posibles situaciones que atenten contra la continuidad del negocio son fundamental. Para lograrlo es necesario que las empresas identifiquen la información crítica para el desarrollo de sus funciones y actividades e incluyan políticas y controles específicos para el manejo de esta información. El estudio emplea como instrumentos de recolección de información, la observación a las instalaciones y centro de Sistemas e Informática, aplicación de entrevistas y aplicación de simulacros, mediante plantillas basadas en estándares internacionales sobre planes de continuidad de negocio.

6.3 Descripción del Plan de Acción

El Plan de Acción tiene como objetivo asegurar que los objetivos o visión de un proyecto se concreten, describe el modo en el que se emplearán las estrategias para alcanzar dichos objetivos y consiste en una serie de pasos a ejecutar, en resumen, el plan de acción es la herramienta para planificar y monitorear actividades (Bussines Continuity Institute, 2010).

La información que se necesita definir en el plan de acción es la respuesta a las siguientes preguntas:

¿Qué cambios o acciones ocurrirán?, ¿Quién hará los cambios?, ¿Cuándo, dónde y durante cuánto tiempo se darán los cambios?, ¿Qué recursos se necesitarán? y a ¿A Quién se deben comunicar los cambios? (Business Connection, 2020)

Es de suma importancia saber que para tener éxito en integrar los principios de continuidad de negocio dentro de Henie Farma se deben tener bien definidas las políticas y procedimientos, todo esto deberá estar principalmente apoyado por liderazgo de la alta gerencia, los responsables de cada área crítica del negocio, capacitaciones y ejercicios de simulación.

El Plan de Acción debe considerar las siguientes aristas respecto a las acciones y tareas: lista de chequeo, una revisión previa, las pruebas de simulación, interrupción completa de los servicios de TI, además es necesario identificar los recursos, responsables, tiempos de ejecución, actividades detalladas y responsables de control de la ejecución.

Es fundamental que todas las unidades o áreas operativas relacionadas con los procesos críticos, puedan intervenir en los simulacros de contingencia que se programen, a fin de evaluar la eficacia de los procedimientos establecidos y estar debidamente capacitados para afrontar cualquier evento y dar una solución rápida, oportuna y simple. Se utilizará el software de Microsoft Office llamado Planner para el control y seguimiento de las actividades a ejecutar.

6.3.1 Objetivo General

Desarrollar un esquema de acciones que permitan evaluar el plan de continuidad del negocio y así poder formalizar, documentar, socializar y readecuar según la necesidad el plan de continuidad, a fin de poder reaccionar o mitigar los riesgos tecnológicos que afectan los procesos críticos de la empresa.

6.3.2 Propósito

Evaluar, readecuar y medir los procedimientos específicos que contienen los procedimientos de recuperación, reanudación y análisis de riesgo del plan de continuidad de Negocios de Henie Farma S. de R. L., para implementar mejoras en sistemas e infraestructura tecnológica relacionada a los procesos críticos del negocio.

6.3.3 Productos

Manual: Plan de Continuidad del Negocio, Henie Farma 2021

6.3.4 Actividades

Ver Anexo 1: Plan de Acción y Cronograma para el Desarrollo del Plan de Continuidad del Negocio Henie Farma 2021



ANEXO 1-Plan de
Acción y Cronogram

6.3.5 Indicadores

- Tiempo máximo tolerable de caída (Maximun Tolerable Downtime por sus siglas en inglés MTD).
- Tiempo Objetivo de Recuperación RTO (Recovery Time Objectives por sus siglas en inglés RTO).
- Punto Objetivo de Recuperación (Recovery Time Objectives por sus siglas en inglés RPO).

Plan de Acción: Plan de Continuidad de Negocio de Henie Farma S. de R. L.

Ver Anexo 1: Plan de Acción y Cronograma para el Desarrollo del Plan de Continuidad del Negocio Henie Farma 2021



ANEXO 1-Plan de
Acción y Cronogram

6.4 Presupuesto

Ver Anexo 2: Presupuesto para el Plan de Continuidad del Negocio Henie Farma 2021-2022



ANEXO
2-Presupuesto para

6.5 Evaluación Financiera

Ver Anexo 2: Presupuesto para el Plan de Continuidad del Negocio Henie Farma 2021-2022



ANEXO
2-Presupuesto para

6.6 Cronograma de Ejecución

Ver Anexo 2: Plan de Acción y Cronograma para el Desarrollo del Plan de Continuidad del Negocio Henie Farma 2021



ANEXO
2-Presupuesto para

6.7 Desarrollo

6.7.1 Identificar Sistemas y Aplicaciones Críticas de TI por Proceso del Negocio

Cuando un sistema o aplicación de TI soporta un proceso crítico del negocio, es decir, un proceso de la empresa, se lo denomina crítico.

Identificar el Tiempo Máximo Tolerable de Caídas (Maximum Tolerable Downtimes por sus siglas en inglés MTD's)

Cuando ya se conocen los procesos críticos del negocio se define el Maximum Tolerable Downtimes (MTD). El MTD indica el tiempo máximo que un proceso del negocio puede estar fuera de servicio.

Identificar el Tiempo Disponible de Recuperación (Recovery Time Objective por sus siglas en inglés RTO)

Indica el tiempo disponible para recuperar los sistemas y recursos una vez ocurrida la interrupción.

Determinar el Punto Objetivo de Recuperación (Recovery Point Objective por sus siglas en inglés RPO)

Es importante determinar la tolerancia que tiene el negocio para la pérdida de datos como resultado de un desastre o interrupción, para esto se define el RTO. RPO (Recovery Point Objective): Es la magnitud de los datos perdidos en términos de un período de tiempo que puede ser tolerado por un proceso del negocio.

Sistemas, Aplicaciones y Servicios Críticos de TI, en Henie Farma.

Tabla 29. Sistemas, aplicaciones y servicios críticos de TI.

Nº	Sistema	DESCRIPCION	PRIORIDAD
1	Intranet	Control de documentación técnica, de comercialización y documentos públicos.	3
2	Gestión de contenidos del sitio web (administrador)	Permite al equipo de Mercadeo gestionar el contenido del sitio web.	2
3	Sistemas de Control de Calidad	Consultar información con control de calidad de los productos fabricados.	1
4	Sistema Contable (Aspel-COI)	Sistema para gestión administrativa	1
5	Sistema Producción (Aspel-Prod)	Sistema para la gestión de insumos, materias primas y producto terminado.	1
6	Sistema de Gestión de Clientes (Aspel-SAE)	Sistema para el control de cuentas por cobrar, por pagar, clientes, inventario.	1
7	Sistema de Conciliación Bancaria (Aspel-BAN)	Sistema contable para la gestión de bancos.	1
8	Sistema de Canjes (Web)	Sistema de registro y visualización de canjes de productos con las cadenas farmacéuticas.	1
9	Sistema de Registro de Visita Médica (Web)	Sistema para registrar y controlar la visita médica.	1
10	PBX	Sistema de gestión de llamadas.	2
11	Sistema de Tickets, Inventario (GLPI)	Sistema para la gestión de inventario y soporte a usuarios.	3
12	Sistema de CCTV	Control de cámaras de seguridad.	2
13	Bases de Datos (MySQL, SQL, Oracle)	Administración de la integridad de las bases de datos.	1
14	Office 365	Sistema de Ofimática	3

N°	Sistema	DESCRIPCION	PRIORIDAD
15	Sistemas Máquinas (Planta Producción)	Sistemas para el control de la maquinaria de producción.	1
16	Sistema de Internet Inalámbrico	Conexión Inalámbrica a la LAN e Internet.	1
17	Enlace de Internet (Tigo)	Internet	1
18	Aplicativo SAE-Móvil	Aplicativo móvil y web para gestión de clientes, cotizaciones, pedidos.	1

Equipos Críticos para los Servicio de TI, en Henie Farma

Tabla 30. Equipos para los servicios críticos de TI

N°	TIPO	MODELO	NOMBRE	FUNCIÓN	PROCESADOR	HDD	RAM	PRIORIDAD
1	Servidor de virtualización	DELL Power Edge R730	SRV-TIC-MINS RV	Servidor Virtual Sistemas ASPEL	12 CPUs x Intel(R) Xeon(R) CPU E5-2687W v4 @ 3.00GHz	1 TB	12 GB	1
				Servidor Virtual Sistema de Canjes	8 vCPUs	1 TB	8 GB	1
2	Servidor Dedicado	DELL Power Edge T110 II S	SRV-ISSABEL	Servidor PBX, GLPI	Intel(R) Xeon(R) E31230 @ 3.2GHz	1 TB	8 GB	1
3	Servidor Dedicado	Clon	SRV-FILES	Servidor de Archivos	8 vCPUs	2 TB	16 GB	2

6.7.2 Análisis del daño que causa la interrupción de un proceso

Es importante determinar las consecuencias de la interrupción de un sistema, recurso o servicio soportado por el departamento de TI con el fin de tener idea del impacto que se produce en el negocio si hay una paralización de operaciones.

6.7.3 Etapas del desarrollo el plan de continuidad del negocio (Aplicabilidad)

La aplicabilidad en su etapa inicial responde esencialmente de la autorización de la gerencia general, sin embargo, el análisis previo de los riesgos, situación actual y propuesta queda al alcance del postulante y a la vez encargado del departamento de TI de Henie Farma S. de R. L. Honduras.

Se identifican las siguientes etapas:

- Evaluación
- Planificación
- Pruebas de viabilidad
- Ejecución
- Recuperación

6.7.3.1 Fase Inicial. (Evaluación)

Con el plan de continuidad del negocio se pretende establecer el lineamiento a seguir para evitar el paro de operaciones (dependientes de los servicios de TI) ante desastres o fallos en los sistemas o servicios de TI, su propone cubrir según ITIL las diferentes etapas del ciclo de vida del plan de continuidad, valorando los servicios y procesos críticos de la empresa.

El alcance del Plan de Continuidad depende también, de los recursos disponibles de la empresa y de las expectativas generadas en su entorno, es importante mencionar que se estipulan procedimientos para dar seguimiento a las estrategias de continuidad y así generar un Plan que siempre pueda estar vigente.

6.7.3.2 Fase 1. Análisis de la empresa (Evaluación)

Su propósito es obtener, elaborar y comprender las circunstancias que rodean a Henie Farma S. de R. L., analizando los procesos, como tecnologías o recursos. Para conseguir estos datos, es necesario realizar ciertas tareas importantes.

Reuniones Multidisciplinarias

Será necesario reunirse con los usuarios asociados con los procesos seleccionados como críticos o que entran dentro de nuestro alcance, recogiendo toda la información sobre el funcionamiento de estos.

6.7.3.3 Análisis de los riesgos (Análisis y Planificación)

Es necesario estudiar y definir las posibles amenazas a las que está expuesta la empresa y el impacto que causarían si estas se producen vulnerabilidades o fallas. Una vez obtenidas las conclusiones basadas en el análisis del riesgo, se realizará un plan de tratamiento de riesgos en el que se describirán medidas, riesgo que mitigar, responsables de la implementación, recursos, etc.

6.7.3.4 Fase 2. Establecer Estrategia de Continuidad (Planificación)

Aquí se determinarán las estrategias de recuperación que se deberán desarrollar para los elementos críticos o que pudieran verse afectados en una contingencia. Esto indica, cómo recuperar

un sistema o un proceso para evitar que la contingencia lo degrade de manera irreversible para la organización.

6.7.3.5 Fase 3. Respuestas (Viabilidad)

Con esta fase se comienza la implantación de la estrategia, aquí se deberá abordar toda la documentación relacionada con la respuesta a la contingencia, para ello es necesario contar con los siguientes documentos:

- Plan de crisis: para el análisis previo a la toma de decisiones.
- Planes operativos de recuperación de entornos: cada proceso o sistema definido como crítico debe tener su plan de recuperación.
- Procedimientos técnicos de trabajo: describen las acciones para la gestión y recuperación de un sistema, infraestructura o entorno.

6.7.3.6 Fase 4. Seguimiento (Ejecución y Recuperación)

Mediante las Pruebas, mantenimiento y revisiones se puede comprobar que el plan de continuidad realmente funciona. para ello, se deben planificar una serie de pruebas sobre los entornos identificados, de los resultados obtenidos se generarán informes donde queden reflejadas todas las incidencias surgidas en el proceso y así establecer medidas correctivas.

6.7.3.7 Fase 5. Socialización (Ejecución y Recuperación)

La socialización es muy importante para fomentar conciencia a los usuarios en general, en materia de continuidad y que conozcan los planes elaborados. El público Meta será el personal técnico y de negocios, si tienen algún tipo de relación con el alcance.

6.8 Definición y Ejecución del Plan de Pruebas (Simulacros)

El plan de pruebas está enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas funcionales, que serán ejecutados por los equipos operativos de Henie Farma, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente esquema:

- Metodología (descripción de la prueba a efectuarse, plantillas de control)
- Alcances (áreas afectadas / personal involucrado, plantilla de control)
- Resultados (Control y certificación de Pruebas)

Las pruebas relacionadas a este plan se deberán ejecutar semestralmente, en los meses de junio y diciembre, con el fin de evaluar la preparación de la entidad, ante la ocurrencia de un siniestro y realizar los ajustes necesarios y deberán ser registradas en el formato detallado en el

Anexo 4.



ANEXO 4 - Control y
Certificación de Sim

Referencias

- Abast Systems & Solutions S.L. (2021). *Plan de Contingencia de TI: Asegurar la disponibilidad*. Obtenido de <http://www.abast.es/ciberseguridad/consultoria-de-seguridad-ti/planes-de-contingencia/>
- Amaya, H. C. (18 de 07 de 2012). *WeLiveSecurity*. Obtenido de <https://www.welivesecurity.com/la-es/2012/07/18/continuidad-negocio-como-responder-ante-emergencia/>
- Business Connection. (1 de 12 de 2020). *Plan de acción x Plan estratégico: comprenda la diferencia*. Obtenido de <https://blog.luz.vc/es/que-es/plan-de-acci%C3%B3n-x-plan-estrat%C3%A9gico-entender-la-diferencia/>
- Bussines Continuity Institute. (2010). *Good Practices Guidelines 2010*. Obtenido de https://www.efectus.cl/upload_files/documentos/20042010092531-112191411.pdf
- CEUPE. (2021). *La infraestructura tecnológica*. Obtenido de <https://www.ceupe.com/blog/infraestructura-tecnologica.html>
- CNBS. (2005). *Circular CNBS No.119/2005*. Tegucigalpa: CNBS.
- CNBS. (2019). *Proyecto de reformas a la norma sobre gestión integral de riesgos*. Tegucigalpa: CNBS.
- CNBS. (03 de 11 de 2020). *CNBS*. Obtenido de <https://www.cnbs.gob.hn/wp-content/uploads/2020/11/CIRCULAR-SBO-NO.-22-2020-Planes-de-Contingencia-y-Continuidad-de-Negocios-ante-Huracan-ETA.pdf>
- Colina, C. L., & Roldán, P. L. (1991). El análisis de componentes principales: aplicación al análisis de datos secundarios. *Revista de Sociología*, 37. Obtenido de <http://www.raco.cat/index.php/Papers/article/download/25101/58447>
- Definición de. (s.f.). *Definición de*. Obtenido de <https://definicion.de/tecnologia-de-la-informacion/>
- Ferrer, R. (16 de 03 de 2010). *Sisteseg Consulting Services*. Obtenido de https://www.sisteseg.com/files/Microsoft_PowerPoint_-_PLANES_DE_CONTINUIDAD_NEGOCIO_V_3.0.pdf
- Garay, J. (09 de 07 de 2013). Obtenido de [http://businesscontinuity-pe.blogspot.com/2012/07/antecedentes-historicos-de-la.html#:~:text=La%20recuperaci%C3%B3n%20ante%20desastres%20\(disaster,organizaciones%20con%20sus%20sistemas%20computarizados.](http://businesscontinuity-pe.blogspot.com/2012/07/antecedentes-historicos-de-la.html#:~:text=La%20recuperaci%C3%B3n%20ante%20desastres%20(disaster,organizaciones%20con%20sus%20sistemas%20computarizados.)
- Garzón-Bejarano, A. (01 de 09 de 2010). *DocPlayer*. Obtenido de <https://docplayer.es/2839068-Tendencias-metodologicas-de-gestion-de-riesgo-informatico-y-continuidad-del-negocio-adelgarzon-bejarano-septiembre-1-de-2010.html>
- Gaviria, C. (2004). *Bitácora Farmacéutica*. Obtenido de <https://bitacorafarmaceutica.files.wordpress.com/2008/08/la-industria-farmaceutica-en-honduras.pdf>

- Gobierno de Alemania. (2006). Desarrollo de Sistemas de Alerta Temprana. *Tercera Conferencia Internacional sobre Alerta Temprana*, 2. Obtenido de https://www.preventionweb.net/files/608_spanish.pdf
- Goh, M. H. (2015). *A Manager's Guide to Implement Your Infectious Disease Business Continuity Plan*. Singapur: BCM Institute.
- Hernandez, F. &. (2010). *Metodología de la investigación*. Ciudad de México: McGraw-Hill.
- Hernández-Sampieri, R. (2018). *Metodología de la Investigación: las rutas cuantitativa, cualitativa y mixta*. Ciudad de México: McGRAW-HILL INTERAMERICANA EDITORES, S.A. de C. V.
- IBM. (04 de 2019). *What is a disaster recovery (DR) plan?* Obtenido de <https://www.ibm.com/services/business-continuity/disaster-recovery-plan>
- IBM Global Technology Services. (2017). Servicios de continuidad de negocio y resiliencia de IBM. *Informe técnico de liderazgo tecnológico*, 1-12.
- ICONTEC. (2009). *NTC-ISO-IEC 27005: Gestión del Riesgo en la Seguridad de la Información*. Bogotá: ICONTEC.
- Incibe. (02 de 01 de 2017). *Pasos a seguir para realizar un análisis de impacto en nuestro negocio*. Obtenido de <https://www.incibe.es/en/node/2687>
- Isaca.Org. (17 de 02 de 2021). *COBIT 5*. Obtenido de <http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx>
- ISO Tools. (16 de 02 de 2021). *ISO 22301*. Obtenido de <https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301>
- ISO.org. (2015). *Sistemas de gestión de la calidad — Fundamentos y vocabulario*. Obtenido de <https://www.iso.org/obp/ui/es/#iso:std:iso:9000:ed-4:v1:es>
- ISOTools. (16 de 02 de 2021). *ISO 27001 - Software ISO 27001 de Sistemas de Gestión*. Obtenido de <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001>
- IsoTools. (2021). *Sistemas de Gestión de Riesgos y Seguridad*. Obtenido de <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001>
- Khan Academy. (2021). *Probabilidad: Conceptos Básicos*. Obtenido de <https://es.khanacademy.org/math/statistics-probability/probability-library/basic-theoretical-probability/a/probability-the-basics>
- Kirvan, P. (14 de 11 de 2013). *Guía de evaluación de riesgos de TI*. Obtenido de <https://searchdatacenter.techtarget.com/es/tutoriales/Guia-de-evaluacion-de-riesgos-de-TI>
- López-León, D. R. (2008). Plan de contingencia para el archivo de la Universidad de La Salle como parte de la implantación del sistema integrado de conservación. *Códice*, 86-89.
- Maldonado, D. (26 de 06 de 2020). *ICORP*. Obtenido de <http://www.icorp.com.mx/blog/rto-y-rpo-recuperacion-ante-desastres/>

- MINTIC. (12 de 05 de 2015). *Guía para realizar el Análisis de Impacto de Negocios BIA*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf
- Mur, A. (02 de 2013). *CriptoRed*. Obtenido de <http://www.criptored.upm.es/descarga/ConferenciaAlfonsoMurTASSI2013.pdf>
- NFPA. (2021). *National Fire Protection Association*. Obtenido de <https://www.nfpa.org/>
- NIST. (2021). *NIST SP 800-34*. Obtenido de <https://www.nist.gov/>
- NU. CEPAL. División de Estadísticas. (2017). *Anuario Estadístico de América Lartina y el Caribe*.
- Ochoa, C. (Citado en 2021). *Muestreo no probabilístico: muestreo por conveniencia*. Obtenido de <https://www.netquest.com/blog/es/blog/es/muestreo-por-conveniencia>
- Polanco, M. (06 de 03 de 2013). *ITIL, CISSP, CISA y CISM*. Obtenido de <https://www.magazcitum.com.mx/?p=2105>
- Proexport-Colombia. (1 de 12 de 2004). *Estudio de Mercado en Honduras*. 1-75. Obtenido de <https://bitacorafarmaceutica.files.wordpress.com/2008/08/la-industria-farmaceutica-en-honduras.pdf>
- Purica, C. A. (03 de 05 de 2018). *Desmitificando los Objetivos de Recuperación*. Obtenido de <https://www.veeam.com/blog/es-lat/rto-rpo-definitions-values-common-practice.html>
- QuestionPro. (2021). *Técnicas de investigación cuantitativa para recolectar datos*. Obtenido de <https://www.questionpro.com/blog/es/tecnicas-de-investigacion-cuantitativa/>
- Redondo, F. (18 de 11 de 2020). *WTW Update*. Obtenido de <https://willistowerswatsonupdate.es/riesgos-corporativos-y-directivos/continuidad-de-negocio-industria-farmaceutica-en-pandemia/>
- Roberto Hernández Sampieri, C. F. (2014). *Metodología de la Investigación*. México D.F.: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.
- Sánchez, F. (01 de 02 de 2002). *Computer World*. Obtenido de <https://www.computerworld.es/archive/bajo-el-efecto-11-de-septiembre-planes-de-continuidad-del-negocio>
- SearchDataCenter. (01 de 01 de 2009). *Proyectar con COBIT e ITIL el plan de recuperación de desastres*. Obtenido de <https://searchdatacenter.techtarget.com/es/consejo/Proyectar-con-COBIT-e-ITIL-el-plan-de-recuperacion-de-desastres>
- Segovia, A. J. (2021). *27001 Academy*. Obtenido de <https://advisera.com/27001academy/es/what-is-bs-25999/>
- SELA. (01 de 08 de 2013). *La continuidad de negocios y operaciones frente a situaciones de desastre en América Latina y el Caribe. Balance y recomendaciones*. Obtenido de https://reliefweb.int/sites/reliefweb.int/files/resources/La%20continuidad%20de%20negocios%20y%20operaciones%20frente%20a%20situaciones%20de%20desastre%20en%20America%20Latina%20y%20el%20Caribe_%20Balance%20y%20recomendaciones.pdf

- SELA. (01 de 01 de 2013). *Sistema Económico Latinoamericano y del Caribe*. Obtenido de <http://www.sela.org/es/>
- Serrano, V. C. (2021). *R para el análisis estadístico de datos*. Obtenido de https://www.uv.es/vcoll/Temas_AED/2_Introduccion.html
- SISTESEG. (2021). *Política de Continuidad del Negocio*. Obtenido de https://www.sisteseg.com/files/Microsoft_Word_-_POL_TICA_DE_CONTINUIDAD_DEL_NEGOCIO.pdf
- Software-GreenHouse. (s.f.). *RPO (Recovery Point Objective)*. Obtenido de <https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo>
- Tamayo, M. T. (2002). *El Proceso de la Investigación Científica*. México D.F.: Editorial Limusa S.A. de C.V.
- TechTarget. (08 de 2014). *Gestión de TI*. Obtenido de <https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-TI>
- UCESI. (01 de 01 de 2020). *Tecnologías para la Enseñanza y el Aprendizaje*. Obtenido de Universidad UCESI: <https://www.icesi.edu.co/servicios/minitab/>
- UCSF. (14 de 07 de 2016). *IT Service Continuity Management*. Obtenido de <https://itsm.ucsf.edu/sites/itsm.ucsf.edu/files/ITSM%20BIA%20Process%20v1.2-1.pdf>
- UJAEN. (2021). *Conceptos:calidad del servicio*. Obtenido de https://www.ujaen.es/servicios/archivo/sites/servicio_archivo/files/uploads/Calidad/Criterio5.pdf
- Valora Data. (26 de 07 de 2018). *Importancia de la Contingencia*. Obtenido de <https://www.valoradata.com/blog/importancia-de-la-contingencia-bcp-y-drp/>
- WeliveSecurity. (14 de 10 de 2014). *¿En qué consiste un Plan de Recuperación ante Desastres (DRP)?* Obtenido de <https://www.welivesecurity.com/la-es/2014/10/14/plan-de-recuperacion-ante-desastres/>