UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA

**PROGRAMA ACADÉMICO DE INGENIERÍA DE REDES Y
COMUNICACIONES**

Diseño de un plan de continuidad para los servicios críticos del área de
Tecnología de la Información de la empresa JJC Contratistas Generales S.A.
basado principalmente en la norma ISO/IEC 27031:2011

TESIS

Para optar el título profesional de Ingeniero de Redes y Comunicaciones

AUTOR

Correa Salazar, Renzo Giancarlo (0000-0003-4494-3206)

ASESOR

Seminario García, Hernán Augusto (0000-0001-6971-355X)

Lima, 20 de marzo de 2019

DEDICATORIA

En primer lugar, a Dios por permitirme cumplir mis objetivos y bendecirme para poder realizar este trabajo; en segundo lugar, a mi hijo y a mi esposa por motivarme a seguir esforzándome y mejorar cada día de mi vida; por último, a mis padres y a mis hermanos por sus enseñanzas y apoyo en todo momento.

RESUMEN

El presente proyecto tiene como objetivo realizar el diseño de un plan de continuidad de servicios críticos de TI basado principalmente en la norma ISO/IEC 27031:2011 y demás guías para la empresa constructora JJC Contratistas Generales S.A. para así tener una mejor capacidad de respuesta ante una interrupción parcial o total de los servicios, así como también lograr una alta disponibilidad con tiempos relativamente cortos de recuperación y poder dar continuidad al negocio.

El trabajo está dividido en cinco puntos que permitirán conocer y entender lo que se diseñará. En el primer punto; se desarrollarán los aspectos introductorios como la situación problemática, los objetivos del proyecto y el estado del arte. En el segundo punto; se detallará el marco teórico que permitirá conocer acerca de los conceptos de plan de continuidad de servicios de TI, su importancia y las fases que tiene. En el tercer punto; se explicará la definición del problema así como el alcance de la solución, la elaboración de los análisis de riesgos, de amenazas y de vulnerabilidades. En el cuarto punto; se realizará la elaboración de la política de continuidad, se realizará la evaluación del riesgo junto con el análisis de impacto de negocio, se desarrollarán las estrategias de continuidad para diferentes escenarios y se detallarán las alternativas de continuidad. Por último, en el quinto punto se realizará el plan de pruebas, la ejecución, la revisión y validación de resultados de las pruebas.

Para finalizar el trabajo, se mostrarán las conclusiones y recomendaciones para futuros proyectos.

Palabras clave: Continuidad; Servicios críticos; Alta disponibilidad; Interrupción; Recuperación; Análisis de riesgos; Análisis de impacto de negocio; Estrategias de continuidad.

Design of a continuity plan for critical services in the area of Information Technology of the company JJC Contratistas Generales S.A. based mainly on ISO/IEC 27031:2011

ABSTRACT

The objective of this project is to design a continuity plan for critical IT services based mainly on ISO/IEC 27031:2011 and other guidelines for the construction company JJC Contratistas Generales S.A. in order to have a better response capacity to a partial or total interruption of the services, as well as to achieve high availability with relatively short recovery times and to be able to continue the business.

The work is divided into five points that will allow knowing and understanding what will be designed. In the first point; the introductory aspects will be developed, such as the problematic situation, the objectives of the project and the state of the art. In the second point; the theoretical framework that will allow to know about the IT service continuity plan concepts, its importance and the phases it has will be detailed. In the third point; the definition of the problem will be explained as well as the scope of the solution, the elaboration of the risk, threat and vulnerability analysis. In the fourth point; the development of the continuity policy will be carried out, the risk assessment will be carried out together with the business impact analysis, continuity strategies will be developed for different scenarios and continuity alternatives will be detailed. Finally, in the fifth point, the test plan, execution, review and validation of test results will be carried out.

To finalize the work, the conclusions and recommendations for future projects will be shown.

Keywords: Continuity; Critical services; High availability; Interruption; Recovery; Risk analysis; Business impact analysis; Continuity strategies.

TABLA DE CONTENIDOS

1	INTRODUCCIÓN.....	1
2	ASPECTOS INTRODUCTORIOS.....	2
2.1	Organización Objetivo.....	2
2.2	Campo de acción en la organización objetivo	2
2.3	Situación problemática	3
2.4	Identificación del problema	4
2.5	Objetivos.....	4
2.5.1	Objetivo general	4
2.5.2	Objetivos específicos	5
2.6	Indicadores de logro de objetivos.....	5
2.7	Justificación del proyecto	6
2.8	Estado del arte	6
3	MARCO TEÓRICO.....	11
3.1	¿Qué es un plan de continuidad?	11
3.2	Importancia del plan de continuidad	12
3.3	Objetivo del plan de continuidad.....	12
3.4	Fases del plan de continuidad.....	13
3.5	Análisis de riesgos	19
3.6	Análisis de impacto de negocio (BIA)	21
3.7	Estrategias de continuidad y alternativas de solución	23
3.8	Tiempos de recuperación y restauración (RTO y RPO).....	24
3.9	Política de continuidad	26
4	DEFINICIÓN DEL PROBLEMA	27
4.1	Análisis de riesgos.....	27
4.1.1	Servicios críticos	27
4.1.2	Dimensiones de valoración.....	30
4.1.3	Criterios de valoración.....	31
4.2	Análisis de amenazas.....	33
4.3	Análisis de vulnerabilidades	35
4.4	Edt.....	39

4.5	Alcance de la solución	40
5	DISEÑO DE LA SOLUCIÓN	42
5.1	Política de continuidad de negocio	42
5.2	Equipo de TI para la continuidad de servicios críticos.....	43
5.3	Evaluación de riesgo.....	43
5.4	Análisis de impacto de negocio (BIA)	45
5.4.1	Identificación de procesos críticos	45
5.4.2	Evaluación de impactos operacionales	46
5.4.3	Establecimiento de tiempos de recuperación.....	48
5.4.4	Impacto económico.....	51
5.5	Estrategias de continuidad	54
5.6	Actividades del equipo de TI en el antes, durante y después de la interrupción de servicios críticos	60
5.7	Lineamientos generales para las alternativas de solución en los diversos escenarios.....	63
5.8	Alerta inicial del plan y plantilla de recuperación	71
5.8.1	Diseño de alerta inicial del plan	71
5.8.2	Plantilla de recuperación	72
6	PRUEBAS, RESULTADOS Y VALIDACIÓN	74
6.1	Pruebas del plan de continuidad	74
6.1.1	Fases y tipos de pruebas	74
6.1.2	Plan de pruebas	75
6.1.2.1	¿Qué se probará?	75
6.1.2.2	Escenarios de pruebas.....	76
6.1.2.3	Modalidad o tipo de prueba	77
6.1.2.4	Fechas de las pruebas	78
6.1.2.5	Personal responsable en las pruebas	78
6.1.3	Ejecución de pruebas	79
6.1.3.1	Para los servidores de archivos.....	79
6.1.3.2	Para el sistema SAP	83
6.1.3.3	Para el correo electrónico	84
6.1.3.4	Pruebas de escritorio.....	91

6.2	Revisión de resultados	96
6.2.1	Análisis y evaluación de resultados.....	96
6.2.2	Evaluación de resultados – Equipo de TI	99
6.2.3	Evaluación de resultados – Usuarios de la organización.....	99
6.2.4	Evaluación de resultados (tiempos) – Servicios críticos de TI.....	100
6.3	Validación de resultados.....	100
7	CONCLUSIONES	105
8	RECOMENDACIONES	106
9	REFERENCIAS	107
10	GLOSARIO.....	109
11	SIGLARIO	111
12	ANEXOS	112

ÍNDICE DE TABLAS

Tabla 1 <i>Indicadores de logro de objetivos</i>	5
Tabla 2 <i>Plantilla MINTIC</i>	22
Tabla 3 <i>Escala de valoración de los servicios de TI</i>	27
Tabla 4 <i>Lista de servicios que brinda el área de TI de JJC Contratistas Generales</i>	28
Tabla 5 <i>Escala de valoración de la probabilidad de ocurrencia de riesgos</i>	31
Tabla 6 <i>Escala de valoración del impacto</i>	32
Tabla 7 <i>Valoración del riesgo</i>	32
Tabla 8 <i>Análisis de amenazas existentes para los servicios críticos de TI</i>	33
Tabla 9 <i>Análisis de vulnerabilidades existentes de los servicios críticos de TI</i>	35
Tabla 10 <i>Matriz de interesados</i>	40
Tabla 11 <i>Requerimientos para el desarrollo del plan de continuidad de servicios</i>	41
Tabla 12 <i>Detalle del equipo de TI para la continuidad de servicios</i>	43
Tabla 13 <i>Evaluación de riesgos</i>	44
Tabla 14 <i>Niveles de criticidad de servicio</i>	46
Tabla 15 <i>Evaluación de impactos operacionales para los servicios críticos de JJC</i>	46
Tabla 16 <i>Descripción de tiempos de recuperación</i>	48
Tabla 17 <i>Prioridades de recuperación de servicios críticos</i>	49
Tabla 18 <i>Disposición de los RPO/RTO por cada servicio crítico</i>	50
Tabla 19 <i>Cálculo de pérdida económica estimada por hora de cada servicio de JJC</i>	52
Tabla 20 <i>Estimación de impacto económico por día para los servicios críticos de JJC</i>	53
Tabla 21 <i>Estrategias de continuidad</i>	55
Tabla 22 <i>Equipo de TI que validará las pruebas de escritorio</i>	91
Tabla 23 <i>Usuarios seleccionados para las pruebas de escritorio</i>	93
Tabla 24 <i>Cantidades de usuarios encuestados por cada área</i>	95
Tabla 25 <i>Respuestas del equipo de TI</i>	97
Tabla 26 <i>Respuestas de usuarios por cada área evaluadas por el equipo de TI</i>	97
Tabla 27 <i>Resultado de identificación y evaluación del riesgo</i>	101
Tabla 28 <i>Impacto operacional de paralización de los tres servicios críticos</i>	102
Tabla 29 <i>Impacto económico de paralización de los tres servicios críticos</i>	102
Tabla 30 <i>Muestra de evaluaciones de estrategias de continuidad con alternativas de solución ante un escenario de paralización</i>	103
Tabla 31 <i>Comparación de tiempos de restauración de los servicios críticos de TI</i>	104

ÍNDICE DE FIGURAS

<i>Figura 1.</i> Evolución de la norma ISO/IEC 27031:2011	9
<i>Figura 2.</i> Concepto de preparación de las TIC para la continuidad del negocio	13
<i>Figura 3.</i> Actividades en las fases del plan de continuidad según el Modelo PDCA	15
<i>Figura 4.</i> Hitos durante un proceso de interrupción.....	25
<i>Figura 5.</i> Balanceo de costos para los tiempos de recuperación.....	26
<i>Figura 6.</i> EDT	39
<i>Figura 7.</i> Evidencia de sincronización de file server en sitio alternativo	80
<i>Figura 8.</i> Evidencia de sincronización de file server en sitio principal	81
<i>Figura 9.</i> Evidencia de correo electrónico enviado por la Mesa de Ayuda de JJC para avisar a los usuarios el corte del sistema SAP. En interno se hará la prueba de continuidad.....	83
<i>Figura 10.</i> Gráfica de monitoreo Cacti para ver la conexión a SAP en servidores alternos de IBM.....	84
<i>Figura 11.</i> Evidencia de replicación de las bases de datos de correo electrónico al sitio alternativo	86
<i>Figura 12.</i> Gráfica de monitoreo Cacti para ver la réplica de las bases de datos de correo electrónico en los servidores alternos que están en Villa el Salvador	87
<i>Figura 13.</i> Evidencia de prueba de restauración semestral de Back-up de Bases de Datos SQL en el mes de Junio del año 2017	88
<i>Figura 14.</i> Gráfica de documentación de estado de Back-ups mensuales (completos) por cada servidor en el año 2017	89
<i>Figura 15.</i> Cuadro de documentación de estado de Back-ups diarios (incrementales) en un mes del año 2017	90

1 INTRODUCCIÓN

Actualmente, la información se ha convertido en el activo principal de las organizaciones y dependen de ella por las operaciones que se realizan; por ello, los servicios de TI tienen un rol importante, de manera que si sufren interrupciones se producen pérdidas de tiempo ya que se tienen que realizar procesos alternos o manuales; pero peor aún, se puede producir pérdidas de dinero.

Muchas empresas peruanas del sector construcción no cuentan con un plan de continuidad para sus servicios críticos de Tecnología de la Información porque consideran que TI (o Sistemas en algunos casos) solo es un área de apoyo, tal como lo son Logística, Gestión Humana, Contabilidad; y no es un área tan crítica como lo son las de Ingeniería, Operaciones, Comercial, etc., a las que sí les brindan la importancia adecuada tanto en sus procesos como en sus recursos humanos.

La Tecnología de la Información en el sector construcción es muy importante para la mejora de la productividad, la reducción de costos y mejoras del proceso constructivo.¹ Ruggirello nos dice que:

“En el sector de la construcción, la difusión de las TIC’S reducen los costos de transacción de los trabajos de gestión y permiten una mayor desterritorialización de las actividades productivas; esto se manifiesta con claridad en las etapas iniciales de ingeniería básica y en el desarrollo de nuevas formas de organización del proceso constructivo.” (Ruggirello 2011:5)

Es por eso que el plan de continuidad de negocio para los servicios de TI se ha convertido en un parte fundamental en las empresas, ya que como su nombre lo indica, garantiza la continuidad de los servicios de Tecnología de la Información en caso de que se presenten problemas o desastres que ocasionen la paralización parcial o total de los sistemas y procesos de vital importancia.

En este caso, para la elaboración y diseño de un óptimo plan de continuidad nos basaremos en las buenas prácticas, controles y métodos que brinda la norma ISO/IEC 27031:2011 para mejorar la disposición de las TIC de la empresa y poder asegurar la continuidad del negocio.

¹ Cfr. Ruggirello 2011: 5

2 ASPECTOS INTRODUCTORIOS

2.1 Organización Objetivo

La organización que tomaremos para desarrollar el proyecto es JJC Contratistas Generales S.A. Esta empresa se dedica al rubro de construcción desde el año 1955. Gracias al buen apogeo que tiene el sector en el mercado peruano ha podido crecer en gran manera y esto le permitió ampliarse internacionalmente a Colombia y a Chile. Como modelo de negocio su actividad principal son los servicios de ingeniería y construcción, concesiones de infraestructura y desarrollo inmobiliario.²

Tiene como principal misión la de satisfacer las expectativas de sus clientes y agregar valor a sus actividades. Su visión es la de ser un grupo empresarial de alcance internacional, que ofrezca servicios diversificados e integrados de ingeniería y construcción, concesiones de infraestructura y desarrollo inmobiliario, basado en la ética de sus profesionales, en su capacidad de gestión e innovación y en la seriedad en el cumplimiento de sus compromisos.³

La empresa cuenta con aproximadamente 250 empleados de oficina y 2000 obreros. Ambas cifras varían de acuerdo a la demanda; es decir, cuando se tiene más obras ganadas, se contrata a más personal y en el caso de no tenerlas, las cifras se reducen.

JJC Contratistas Generales S.A. tiene una oficina principal ubicada en el distrito de Miraflores, un almacén central ubicado en el distrito de Villa el Salvador y diversas Obras tanto en Lima como en provincias. La conexión entre la oficina principal y el almacén central se establece a través una red privada virtual con el ISP Claro.

2.2 Campo de acción en la organización objetivo

El campo de acción en la organización será el área de la Gerencia de Tecnología de la Información que cuenta con un Centro de Datos principal ubicado en la oficina principal (Miraflores) y con uno secundario ubicado en el almacén central (en Villa el Salvador). Esta área tiene como objetivo proporcionar soluciones basadas en las tecnologías de la información para la mejora continua de los procesos del negocio y soportar el crecimiento de éste.

² Cfr. JJC 2016

³ Cfr. JJC 2016

La Gerencia de TI brinda diversos servicios como el sistema ERP (SAP), facturación electrónica, sistema de presupuestos (S10), sistema gestor de licenciamiento de AutoCAD, sistema gestor de proyectos, repositorios de red para compartir archivos (File Servers), correo electrónico, telefonía IP, conexión VPN, etc.

De todos los servicios mencionados, junto con la alta gerencia y el área de TI se han definido tres como los más críticos: los servidores de archivos, el sistema ERP y el correo electrónico.

1. Servidores de archivos: La información actual e histórica de las diversas licitaciones ganadas o las que ha participado JJC tanto para el área de Ingeniería que contiene presupuestos, planos y metrados, así como para el área Comercial que tienen almacenadas las presentaciones y acuerdos con los clientes es considerada de vital importancia. Sin embargo, se considera también toda la información en los File Servers (plataforma Microsoft) de las demás áreas como la Gerencia General, Administración, Finanzas, Contabilidad, Consorcios, Planeamiento, Seguridad, Logística, Gestión Humana, etc. como importante, ya que todo forma parte del flujo de información y desarrollo de procesos que tiene la organización.
2. Sistema ERP: JJC considera el sistema SAP R/3 como el principal gestor de la información en las operaciones de la empresa. Es utilizado en la oficina principal, en el almacén central y en todas las obras para unificar diversos procesos. Además, es el sistema principal que tiene los procesos contables y de facturación, de almacenes, logísticos, planilla de trabajadores, etc.
3. Correo Electrónico: En JJC este servicio (bajo Exchange Server 2013) es considerado como crítico porque se utiliza como la vía más rápida para realizar coordinaciones internas y externas, contactar a los clientes y compartir información con ellos. Lo mismo para los proveedores y personal en obra.

2.3 Situación problemática

La situación problemática que se da en JJC Contratistas Generales S.A. es que en la actualidad se genera lentitud en determinados periodos de tiempo, incluso ocurren paralizaciones por diferentes causas en los servicios que brinda TI incluyendo los más críticos que se han definido en el campo de acción, ya sea por falla de software/hardware en algún servidor del Centro de Datos principal, por saturación de ancho de banda o caída de enlace entre los Centros de Datos, etc. Existen procesos para garantizar la disponibilidad en

los principales servicios como la replicación de algunos servidores entre la oficina principal y el almacén central, pero de igual forma aún no es posible mantenerlos estables y continuos de un modo tolerable por la organización.

También, por diversos motivos (sea error de usuario, por algún malware, por problema de hardware o por algún error de administración en la red) se borra información; y entonces se presenta demora en la restauración de información que además, en varios casos no es posible la recuperación por completo.

Con estas situaciones expuestas, principalmente se puede producir la pérdida de alguna licitación en la que participa la empresa. La preparación de la oferta que se presentará al cliente es considerada lo más crítico por ser el punto de partida para generar ingresos a la organización. Además, se ocasiona una incomodidad en los usuarios la cual presentan sus quejas en las encuestas semestrales que realiza la Gerencia de TI para medir el servicio brindado a la organización; esto último mencionado se da más por las interrupciones de los servicios y las demoras en los restablecimientos.

2.4 Identificación del problema

El problema identificado es que no se mantienen los servicios estables y continuos para los usuarios de la organización por las paralizaciones periódicas que ocurren. Pueden haber caídas en los servicios, pero no existen alternativas de solución para la continuidad que maneje tiempos tolerables de restablecimiento de servicios para JJC y además no se administran correctamente las copias de seguridad de la información (Back-up) que son fundamentales en el caso de perder algún servicio; algunas veces es incompleta la restauración o en el peor de los escenarios no se puede realizar porque falló la copia inicial.

2.5 Objetivos

2.5.1 Objetivo general

Diseñar un plan de continuidad para los servicios críticos del área de Tecnología de la Información de la empresa JJC Contratistas Generales S.A. basado principalmente en la norma ISO/IEC 27031:2011 que permita proponer alternativas de continuidad para soportar los procesos de negocio en caso de ocurrir incidentes.

2.5.2 Objetivos específicos

- a. Identificar los riesgos de continuidad que podrían afectar los servicios críticos del área de Tecnología de la Información según el punto 6.3.2 Comprensión de los Servicios Críticos de las TIC de la norma ISO/IEC 27031:2011.
- b. Desarrollar el análisis de impacto de negocio para poder determinar los impactos operacionales e impacto económico referente a los servicios críticos según los lineamientos del anexo B del NIST SP 800-34 Rev. 1.
- c. Establecer estrategias de recuperación y restauración de los servicios críticos del área de TI según el punto 6.4.2 Opciones Estratégicas de la norma ISO/IEC 27031:2011.
- d. Determinar periodos de recuperación requeridos por la organización para la continuidad de los servicios críticos del área de TI según los puntos 6.4.2.4 Datos y 7.4 Documentos del Plan de la norma ISO/IEC 27031:2011.

2.6 Indicadores de logro de objetivos

Tabla 1

Indicadores de logro de objetivos

OBJETIVO ESPECÍFICO	INDICADOR DE LOGRO	MÉTRICA
a. Identificar los riesgos de continuidad que podrían afectar los servicios críticos del área de Tecnología de la Información.	Matriz de escenarios de amenazas, valoración de riesgos, probabilidades de ocurrencia e impacto (ver Anexo 1) que tienen en los servicios críticos de TI.	Niveles de criticidad de los servicios críticos.
b. Desarrollar el análisis de impacto de negocio para poder determinar los impactos operacionales e impacto económico referente a los servicios críticos.	Matriz BIA.	Pérdidas económicas estimadas por caída de servicios críticos.
c. Establecer estrategias de recuperación y restauración de los servicios críticos del área de TI.	Matriz de estrategias de continuidad (comparar beneficios, impacto, costos, etc.)	Estrategias de continuidad de recuperación rápida para los servicios de la organización.
d. Determinar periodos de recuperación requeridos por la organización para la continuidad de los servicios críticos del área de TI.	Matriz de niveles de servicio requeridos. Tiempos propuestos aceptados por la organización.	RTO y RPO de los servicios críticos. Reducción aproximada de 65 a 75% de tiempo.

Fuente: Elaboración propia

2.7 Justificación del proyecto

La principal justificación para el desarrollo de este proyecto es que JJC Contratistas Generales S.A. cuenta con dos Centros de Datos (principal y secundario) donde se pueden establecer alternativas de solución que brinden continuidad a sus servicios críticos a través de la alta disponibilidad.

El detalle está en que los dueños y directivos de la empresa son muy celosos con su activo principal que es la información. Siempre solicitan evitar gestionar trabajos y copias de seguridad en la Nube o con un proveedor de Hosting y/o Housing. Es por eso que el diseño de este plan de continuidad tiene una oportunidad de ponerse en marcha y demostrar que sí se puede realizar sobre la estructura actual de TI, siendo la infraestructura escalable en sus dos Centros de Datos para aplicar mejoras.

Con este proyecto, la organización objetivo tendrá resultados favorables y provechosos para su crecimiento ya que podrán ocurrir situaciones inesperadas que paralicen los servicios de TI que gestionan su activo principal (como por ejemplo que se produzca una falla en un servidor de archivos que contenga metrados de planos y presupuestos para una licitación en proceso), pero estará preparada para reaccionar y restablecer sus operaciones en tiempos óptimos que no le generen pérdidas de información y lo más importante, de dinero.

2.8 Estado del arte

Referente al plan de continuidad de negocio:

La continuidad de negocio, en este caso relacionado a los servicios de TI, es un concepto que apareció en los años setenta, dado que los administradores de centros de datos comenzaron a darse cuenta que sus empresas dependían cada vez más de los sistemas informáticos. Dichos sistemas eran ejecutados en grandes servidores de la época, que muchas veces paralizaban sus servicios por muchos días y se generaban pérdidas de dinero.

Con el paso del tiempo, crecía la preocupación sobre tener un plan de recuperación ante desastres o de contingencia que garantice continuidad de las operaciones de los sistemas. Los centros de datos se consideraban los únicos puntos de posibles fallas. Las áreas de TI de las empresas en diferentes países necesitaban de una metodología que no solo permita recuperarse ante desastres sino también que tenga procedimientos y procesos que reduzcan los tiempos de recuperación. Sun Information Systems que luego se convirtió en Sungard

Availability Systems, fue uno de los primeros proveedores de recuperación de desastres de centros de datos y actualmente es uno de los más importantes proveedores de servicios de producción de TI y recuperación en Estados Unidos. El costo de dichos servicios era menor que el costo asumido por el cliente para duplicar su infraestructura informática. Por eso, esta estrategia se convirtió en el estándar para la recuperación de TI desde fines de los años setenta y hoy continúa siendo un importante servicio.

En los años ochenta y noventa, la conciencia acerca de la recuperación tecnológica ante desastres creció muy rápido, debido a que ya existían más empresas que ya tenían un sistema implementado dentro de su organización. Estas empresas se dieron cuenta que tener alguna interrupción de TI traería un impacto negativo en la continuidad de las operaciones que afectan al negocio y sobre todo en los procesos críticos.

Con el crecimiento del Internet en los años noventa y en la década del 2000, las organizaciones de todos los tamaños se volvieron más dependientes de la disponibilidad de sus sistemas informáticos. Algunas empresas establecieron niveles de disponibilidad de hasta 99.99%. Este incremento de la dependencia con los sistemas de TI, así como la conciencia de posibles desastres a gran escala, como el del "11 de septiembre" (ataque a las torres gemelas en Estados Unidos) contribuyeron al crecimiento de las diversas industrias relacionadas a la recuperación ante desastres desde soluciones de alta disponibilidad hasta infraestructuras de sitios alternos y a la consolidación de la disciplina de continuidad de negocios.⁴ Actualmente, el plan de continuidad de servicios críticos de TI engloba todas las funciones y recursos que busca identificar, analizar y evaluar riesgos de posibles amenazas para luego elaborar estrategias que permitan minimizar las caídas y paralización de operaciones de los sistemas informáticos en las organizaciones. Es un elemento clave dentro del gran escenario de la continuidad del negocio.⁵

Un caso de éxito de un plan de continuidad de servicios es la Implementación del Marco de Trabajo de Continuidad de la Infraestructura de TI de ARANDU (Red Académica Paraguaya) que se encarga de interconectar a las universidades y centros de investigación de Paraguay. En el año 2012 desarrollaron un plan de forma seria y responsable ante los desafíos que propone una contingencia y los requerimientos de los usuarios. Los que diseñaron dicho plan, eran conscientes que durante las operaciones cotidianas que realiza ARANDU podían

⁴ Cfr. Garay 2012

⁵ Cfr. Garay 2012

ocurrir situaciones que afecten la normal provisión de servicios; es por eso que, nació este plan para afrontar y superar las diferentes emergencias que sucedieran.⁶

Para garantizar que la infraestructura de Tecnología de Información de ARANDU pueda continuar suministrando servicios (especialmente aquellos considerados críticos) o puedan ser recuperados en un tiempo adecuado en caso de que se produzca una interrupción, fue elaborado un Marco de Trabajo de Continuidad de la Infraestructura de TI, conteniendo las Políticas de Seguridad y el Plan de Contingencias.⁷

La norma ISO 22301 al igual que las otras normas o modelos que veremos más adelante en el diseño del plan, también está basada en el modelo PDCA (Plan – Do – Check – Act) referente a la planeación, establecimiento, implementación, operación, monitoreo, revisión, ejercicios, mantenimiento y mejoramiento de la efectividad para la continuidad de servicios en una organización⁸; fundamentalmente para que la gestión de continuidad se encuentre documentada y preparar a la empresa a responder y recuperarse oportunamente de interrupciones.

Contar con un plan de continuidad significa preparar adecuadamente a la organización para enfrentar cualquier eventualidad, garantizando la provisión de servicios, salvaguardando los intereses de sus miembros, su reputación y las actividades creadoras de valor.⁹

Referente a las normas utilizadas:

La norma ISO/IEC 27031:2011 que tomaremos como base para el desarrollo del diseño del plan de continuidad de servicios críticos en este proyecto describe los conceptos y lineamientos a seguir para mejorar las Tecnologías de la Información y la Comunicación (TICs) para asegurar la continuidad del negocio.¹⁰

El origen de la norma se da en el año 2006 cuando el British Standards Institution (BSI) publicó, en colaboración con diversas empresas del sector TI, un documento que era el BS 25999-1, como código de buenas prácticas para crear un plan de continuidad de servicios de TI. Luego vino el estándar BS 25777 como código de buenas prácticas sobre cómo abordar la gestión de la continuidad de servicios TI en una organización y se especificaría los

⁶ Cfr. Filippi y Serafini 2012: 2

⁷ Cfr. Filippi y Serafini 2012: 2

⁸ Cfr. ISO 22301 2012: 4

⁹ Cfr. Filippi y Serafini 2012: 14

¹⁰ Cfr. ISO 27031 2011: 1

requisitos para establecer, implementar, operar, supervisar, revisar, probar, mantener y mejorar un sistema de gestión de continuidad de servicios TI, además de permitir auditar y certificar los sistemas de gestión de las organizaciones.

El BS 25777 proporciona recomendaciones para la implementación de la continuidad efectiva de las TIC en el marco más amplio de Gestión de Continuidad de Negocio, mientras que la ISO/IEC 27031:2011 fue originalmente destinada a ser un estándar de varias partes, pero finalmente fue reducida a una sola parte como guía.

Figura 1. Evolución de la norma ISO/IEC 27031:2011

Fuente: Elaboración propia

La norma ISO/IEC 27031:2011 es una norma no certificable. Es una guía de apoyo para la adecuar las tecnologías de información y comunicación (TIC) en una organización para garantizar la continuidad del negocio; toma como referencia principalmente el estándar BS 25777 (British Standard).

Esta norma está vinculada con otras normas y estándares que también ayudarán al desarrollo del diseño propuesto:

- ISO 22301:2012 – Sistema de Gestión de Continuidad del Negocio
- NIST SP 800-34 Rev. 1 – Guía de Plan de Contingencia para los Sistemas de Información
- ISO/IEC 27001:2013 – Sistema de Gestión de Seguridad de la Información

- ISO 22398:2013 - Guía para establecer, implementar y mantener un análisis de impacto de negocio (BIA)
- ISO 22317:2015 – Guía para pruebas y validaciones

Cada una de las normas mencionadas, aportan lineamientos importantes para el desarrollo del plan, por ejemplo la metodología para la continuidad de negocio y servicios de TI, algunos controles a tener en cuenta sobre seguridad de la información, guía para la elaboración del BIA, y por último una guía para las pruebas del diseño del plan.

Además debemos resaltar que la norma ISO/IEC 27031:2011 va orientada exclusivamente a la continuidad del negocio relacionado a las TICs a diferencia de la ISO/IEC 22301:2012 que habla de la continuidad del negocio pero desde un marco organizacional.

3 MARCO TEÓRICO

3.1 ¿Qué es un plan de continuidad?

El plan de continuidad está conformado por una serie de procedimientos documentados que guían a las organizaciones a responder, recuperar, reanudar y restaurar a un nivel predefinido de funcionamiento tras alguna interrupción que ocurra. Normalmente, esto cubre los recursos, servicios y actividades que se requieren para asegurar la continuidad de los servicios críticos de TI brindados.¹¹

Tiene que ver también con la capacidad de los elementos de las TIC de una organización para apoyar las funciones críticas del negocio a un nivel aceptable dentro de un período de tiempo predeterminado después de una interrupción.¹²

La Universidad Francisco de Paula Santander define un concepto muy claro: “el plan de contingencia viene a ser una estrategia planificada que cuenta con una serie de procedimientos que facilitan tener una solución alternativa y que permitan restablecer rápidamente los servicios de la organización ante un evento que pueda paralizar o detener los procesos de forma parcial o total.” (UFPS 2015:7)

Además la UFPS define conceptos importantes a tener en cuenta relacionados al plan de continuidad. Estos son los siguientes:

- Ataque: término usado para cualquier evento o acción que intente interferir con el buen funcionamiento de los servicios del área de Tecnología de Información.
- Incidente: ocurre cuando una amenaza se llega a concretar, por ejemplo cuando ocurren fallas eléctricas dentro de la empresa.
- Integridad: se refiere a que toda la información del área de Tecnología de la Información se mantenga tal como estaba desde un principio.
- Continuidad: se refiere a que los sistemas de información puedan mantenerse estables después de haber transcurrido un incidente.

Todas las definiciones mencionadas son importantes en este tema, pero se debe resaltar el concepto de continuidad ya que es fundamental (objetivo principal) de todo plan de continuidad, recuperación de desastres y contingencia. En el caso de los servicios críticos de

¹¹ Cfr. ISO 27031 2011: 2

¹² Cfr. ISO 27031 2011: 3

TI en la empresa JJC Contratistas Generales S.A., se debe apreciar el hecho de darles alta disponibilidad a los servicios ya que de ellos depende la continuidad del negocio.

3.2 Importancia del plan de continuidad

El proceso de continuidad de negocio referente a la Tecnología de la Información, se refiere a un sistema de gestión que complementa y apoya un Plan de Continuidad de Negocio de la organización y/o programa de SGSI.¹³ La importancia de este proceso para mejorar la disposición de la organización referente al plan de continuidad se detalla en los siguientes puntos:

- a) Responder inmediatamente al entorno de riesgo en constante cambio.
- b) Garantizar la continuación de las operaciones críticas de negocio con el apoyo de los servicios de las TIC relacionados.
- c) Estar preparados para responder antes de que ocurra una interrupción del servicio TIC, tras la detección de uno o una serie de relacionados eventos que se convierten en incidentes.
- d) Responder y recuperarse de incidentes / desastres y fracasos.

3.3 Objetivo del plan de continuidad

Todas las actividades de preparación del plan tienen como objetivo los siguientes ítems:¹⁴

- a) Mejorar la capacidad de detección de incidentes.
- b) Evitar un fallo repentino o drástico.
- d) Acortar aún más el tiempo de recuperación.
- e) Minimizar el impacto sobre la eventual ocurrencia del incidente.

¹³ Cfr. ISO 27031 2011: 3-4

¹⁴ Cfr. ISO 27031 2011: 4

Figura 2. Concepto de preparación de las TIC para la continuidad del negocio

Fuente: Norma ISO 27031:2011

Este gráfico nos muestra cómo con la preparación de las TIC en el plan de continuidad se mejora la curva de capacidad de respuesta (restablecimiento de servicios críticos) ante un incidente que origine una paralización.

3.4 Fases del plan de continuidad

Según la norma ISO/IEC 27031:2011, nos sugiere establecer el modelo PDCA (Plan, Do, Check, Act) para las fases del plan de continuidad. Esto implica que la organización establezca los procesos necesarios para desarrollar y mejorar los elementos clave del iRBC (ICT Readiness for Business Continuity) para mejorar su capacidad de responder a cualquier tipo de interrupción, incluidas las situaciones de riesgo cambiantes.¹⁵

¹⁵ Cfr. ISO 27031 2011: 8

La norma nos sugiere de manera general las siguientes fases:

Primera Fase – Planeación del iRBC: (PLAN):

En esta fase se debe realizar una planeación y organización previa para mejorar la capacidad de respuesta ante cualquier tipo de interrupción, incluidas las situaciones de riesgo cambiantes. Aquí se realiza la definición de estrategias.

Segunda Fase – Implementación y Operación (DO):

Las estrategias definidas en la fase de planeación deben ser implementadas tras la aprobación de la alta dirección. En este punto la etapa de ejecución comienza y es necesario tener planes y procedimientos necesarios para apoyar la implementación.

Se deben gestionar los recursos y los procedimientos, así como implementar programas de formación y sensibilización del personal de la organización. La implementación debe ser gestionada como un proyecto a través del control de los procesos de gestión de cambios y gestión de proyectos formales con el fin de garantizar la plena la visibilidad de la gestión y elaboración de informes.¹⁶

Tercera Fase – Monitoreo y Revisión (CHECK):

En esta fase se debe establecer un proceso para monitorear continuamente y detectar la aparición de amenazas para la seguridad de las TIC.

La organización debe asegurarse de que el plan de continuidad se revisa a intervalos planificados. Se puede tener en cuenta además realizar auditorías internas o externas.

Los resultados de la revisión deben ser claramente documentados y los registros deben guardarse.

¹⁶ Cfr. ISO 27031 2011: 15

Cuarta Fase – Mejora del iRBC (ACT):

La organización debe mejorar continuamente plan de continuidad de servicios a través de la aplicación de acciones preventivas y correctivas que son apropiadas para los impactos potenciales determinados por análisis de impacto en el negocio y el apetito por el riesgo.¹⁷

Figura 3. Actividades en las fases del plan de continuidad según el Modelo PDCA

Fuente: Norma ISO 27031:2011

En este modelo se muestra de manera detallada las actividades realizadas en cada fase.

Por otro lado, el NIST (*National Institute of Standards and Technology*) también nos brinda un modelo para establecer las fases del plan de continuidad.

Desde el inicio del documento nos da un claro concepto de que en el plan de continuidad y contingencia de TI se debe definir una política que contenga las funciones y responsabilidades, las copias de seguridad, el desarrollo del plan, las fases de pruebas y el mantenimiento de dicho plan. También nos brinda lineamientos como que el plan se debe

¹⁷ Cfr. ISO 27031 2011: 28

mantener actualizado para que resulte óptimo y beneficioso. Además se deben realizar pruebas de control al menos una vez al año:

“Un plan de contingencia actualizado es esencial para el éxito de las operaciones. Como regla general, el plan de contingencia de TI se debe revisar con exactitud e integridad al menos anualmente. (...) Las deficiencias identificadas a través de pruebas deberán dirigirse durante el mantenimiento del plan. Deben ser revisados y actualizados con mayor frecuencia. Los programas de mantenimiento deben ser expresados en la declaración de política del plan.” (NIST 2010: Appendix C-4)

Por último, el INEI (*Instituto Nacional de Estadística e Informática*) al igual que el NIST, brinda una guía que muestra el ciclo (o fases) del desarrollo del plan de contingencia y continuidad. Esta guía recomienda las siguientes fases:

1. La planificación, donde se define y prepara el esfuerzo para la planificación de continuidad y contingencia¹⁸. En esta fase se debe tener en cuenta el alcance que tendrá el plan, las fases en que se desarrollarán (no en todos los casos necesariamente se tienen que realizar las ocho fases), las responsabilidades de todos los involucrados en la realización del plan, entre otras.

La guía recomienda en la planificación principalmente los siguientes ítems: “Identificación y asignación de los grupos de trabajo iniciales; definición de los roles y responsabilidades. Definición de las partes más importantes de un cronograma maestro y su patrón principal. Identificación de las fuentes de financiamiento y beneficios del negocio; y la revisión del impacto sobre el negocio.” (INEI 2001: 17)

2. La identificación de riesgos, que busca minimizar las fallas que se pueden dar frente al desempeño normal. “El objetivo principal de esta fase es realizar un análisis de impacto económico, determinar el efecto de fallas de los principales sistemas de información y producción de la empresa.” (INEI 2001: 17)

“Es necesario el reconocimiento y reducción de riesgos potenciales que afecten a los servicios, por eso en el plan de continuidad se considera como primer paso la reducción de riesgos que favorecen los objetivos institucionales.” (INEI 2001: 18)

¹⁸ Cfr. INEI 2001: 14

En esta fase se realiza el análisis y evaluación de riesgos así como la identificación de los servicios críticos del área de TI. Además, se debe tener en cuenta el uso de técnicas para análisis de procesos, que ayudarán a la identificación de riesgos.

3. La identificación de soluciones, porque el plan no puede quedar solo en papel y se debe implementar, probar y mejorar.¹⁹

Para esta fase, se debe tener en cuenta la identificación de alternativas de solución como por ejemplo si falla el sistema principal de la organización, los trabajadores deben conocer procesos sobre cómo realizar una factura o un cheque manualmente o también si se corta la energía eléctrica pública, se debe tener generadores de energía o grupos electrógenos.²⁰

Referente a los servicios críticos de TI en la organización objetivo, el área de Tecnología de la Información debe tener presente la mayoría de soluciones a posibles incidentes como pueden ser ataques genéricos a sistemas operativos, seguridad en redes, protección de servidores como arreglo de discos, etc.²¹

Un modo muy práctico para llegar a identificar una alternativa de solución es “no haga nada y vea qué pasa – esta estrategia es algunas veces llamada arreglar sobre falla”. (INEI 2001:22) Esto quiere decir que si falla algún servicio, se podría esperar a ver cómo se reacciona ante el incidente y en base a ello, se tomará alguna solución.

4. Las estrategias, que “están diseñadas para identificar las prioridades de los servicios críticos”. (INEI 2001:34) Aquí se decide si se optarán por soluciones a gran escala o dependiendo de lo que la empresa decida hasta dónde será el alcance del plan (ver costo / beneficio).

En las estrategias podemos poner como ejemplo la administración de cintas de Back-up de los servidores de la organización objetivo. La guía del INEI especifica un ítem referente a ello:

“4.3.1.1 Respecto a la Administración de la Cintoteca:

- Debe ser administrada bajo la lógica de un almacén. Esto implica ingreso y salida de medios magnéticos (sean cintas, disquetes cassettes, cartuchos, Discos removibles, CD's, etc.), obviamente teniendo más cuidado con las salidas.

¹⁹ Cfr. INEI 2001: 21

²⁰ Cfr. INEI 2001: 22

²¹ Cfr. INEI 2001: 26-33

- La cintoteca, que es el almacén de los medios magnéticos (sean cintas, disquetes cassettes, cartuchos, Discos removibles, CD's, etc.) y de la información que contienen, se debe controlar para que siempre haya determinado grado de temperatura y de la humedad.
- Todos los medios magnéticos deberán tener etiquetas que definan su contenido y nivel de seguridad.
- El control de los medios magnéticos debe ser llevado mediante inventarios periódicos.” (INEI 2001:37)

Para el tema del Back-up en cintas magnéticas como estrategia del plan de continuidad se debe considerar varios aspectos como que se deben guardar las cintas de manera adecuada; es decir, mantener niveles de humedad, temperatura, deben estar inventariadas, mantener fuera de campos magnéticos²² y de ser posible mandarlas a un proveedor custodio.

Hay que recordar que la información es el activo más importante que tiene la empresa.

5. La documentación del proceso, que debe ser eficientemente hecha.²³

Esta fase va orientada a la documentación a detalle y además a la difusión de todo lo realizado para el plan de continuidad. Debe ser transmitida a todo el personal de la organización con los puntos más importantes.

6. La realización de pruebas y validación, que se da antes de que ocurra un evento o incidente. Para esta fase se debe definir los procedimientos y planes de acción ante una posible falla en el área de TI. Es esencial conocer al detalle el motivo que originó el incidente y el daño que produjo para que se pueda restablecer los servicios críticos en el menor tiempo posible.²⁴

Aquí podemos clasificar tres etapas: actividades previas al desastre, donde se ve la preparación, entrenamiento, definición de políticas y ejecución de actividades de copias de seguridad de la información²⁵ y colocación de grupos electrógenos para contingencia eléctrica. Luego tenemos actividades durante el desastre, que una vez presentado el siniestro se establecen acciones como puesta a buen recaudo de los activos de información, vías de salida o escape y secuencia de llamadas al personal calificado²⁶ (por ejemplo llamar al Operador de Data Center cuando ocurra un

²² Cfr. INEI 2001: 38

²³ Cfr. INEI 2001: 42

²⁴ Cfr. INEI 2001: 42

²⁵ Cfr. INEI 2001: 43

²⁶ Cfr. INEI 2001: 48

incendio en el Centro de Datos). Por último actividades después del desastre, donde se evalúan los daños ocurridos, la priorización de actividades de restablecimiento de servicios y la retroalimentación del plan de continuidad.²⁷

7. La implementación, que se da cuando ha ocurrido ya el evento o incidente y se tiene que tener listo el plan para aplicarlo. Esta fase también puede tratarse como una prueba controlada.²⁸ Pueden haber emergencias físicas como lo son desastres naturales, incendio, falla en los equipos tecnológicos (servidores, equipos de comunicación, equipos de cómputo finales) o fallas en el fluido eléctrico. También emergencias lógicas como errores en sectores de los discos duros de los servidores, caída de los servidores de archivos, propagación de virus en la red, etc.²⁹

Todo lo mencionado se puede dar en la fase de implementación y el plan de continuidad para los servicios críticos de TI debe estar preparado para cada uno, ya que no es posible saber cuál y cuándo se darán.

8. El monitoreo, que brinda la seguridad de poder reaccionar en el tiempo exacto junto con la acción idónea. Se pueden realizar principalmente las siguientes actividades: establecer los procedimientos de mantenimiento para la documentación y la rendición de informes referentes a los riesgos; revisión constante de las aplicaciones y la revisión constante del sistema de Back-up.³⁰

Esta fase es la última en todo el proceso del plan de continuidad ya que aquí se revisa y monitorea cada parte de dicho plan. Va de la mano con la fase de pruebas y mantenimiento porque en caso de demorar mucho en el restablecimiento de un servicio o que un grupo de trabajo no sepa cómo actuar ante cierto evento, aquí se definirá qué acción tomar para mejorar el plan.

3.5 Análisis de riesgos

Para poder hablar de los riesgos que existen dentro del área de Tecnología de la Información en una empresa peruana de construcción en la actualidad, se debe comenzar definiendo qué es un riesgo en el ámbito empresarial y de TI. Según Montero, en su tesis nos plantea que: “el riesgo es inherente a todo lo que se hace, se convive con él todos los días aunque no se

²⁷ Cfr. INEI 2001: 49

²⁸ Cfr. INEI 2001: 50

²⁹ Cfr. INEI 2001: 51-54

³⁰ Cfr. INEI 2001: 55

esté consciente de ello. Aunque siempre se piensa en desastres, el riesgo más común que las empresas enfrentan, es el de no cumplir con sus objetivos y metas.” (Montero 2011:13)

Se debe considerar para qué sirve evaluar los riesgos. El objetivo de la evaluación del riesgo es identificar, analizar, medir y prevenir las amenazas internas y externas que podrían causar la paralización total o también interrupciones temporales de los servicios de la organización, la cual permite priorizar los servicios e implementar un plan de continuidad.³¹

También es importante definir una amenaza como lo plantea la UFPS: es cualquier cosa que pueda interferir con el funcionamiento adecuado de un equipo informático o servicio, que pueda causar la difusión no autorizada de información confiada en un servidor. Ejemplo: Fallas de suministro eléctrico, virus, sabotadores o usuarios descuidados. (UFPS 2015:6)

Cabe mencionar que un riesgo es el resultado de que una amenaza se concrete al existir una vulnerabilidad.

Montero nos brinda además conceptos clave relacionados al riesgo como:

1. El análisis: se debe comprender y entender los riesgos para lograr saber cómo tratarlos de manera costo-efectiva.³²
Este análisis involucra: la probabilidad de ocurrencia del riesgo, que nos indica la seguridad de que un riesgo se pueda concretar; la determinación del impacto potencial, que nos indica las consecuencias que se pueden generar por la ocurrencia del riesgo; el análisis de riesgos, mediante una combinación de impacto y probabilidad de ocurrencia; y por último, la magnitud de un riesgo que es determinada por su probabilidad de ocurrencia y sus consecuencias o impactos asociados. (ver Anexo 1)
2. La evaluación: consiste en la toma de decisiones basadas en el análisis realizado anteriormente; es decir, definir su prioridad y darles algún tratamiento.³³ Aquí se define a qué servicios críticos se les dará un tratamiento de riesgos.
3. El tratamiento: involucra preparar planes y estrategias para tratar los riesgos.³⁴

³¹ Cfr. Montero 2011: 10

³² Cfr. Montero 2011: 17

³³ Cfr. Montero 2011: 19

³⁴ Cfr. Montero 2011: 21

Para el tratamiento del riesgo se debe considerar en primer lugar la factibilidad; es decir, medir en qué grado es factible tratar el riesgo e intentar reducirlo. También están los costos ya que, puede ser posible reducir el riesgo, pero esto llevará a invertir mucho dinero y en algunos casos se tiene que definir un tope de gastos. Los beneficios se tienen que medir luego de ver la factibilidad y los costos, porque puede ser factible reducir riesgos, invertir mucho o tal vez poco dinero para hacer esto, pero no nos dará mucha ventaja realizar todo este esfuerzo, en ese caso, no debería realizarse el tratamiento de riesgo y se deben elegir otros.

En la fase de tratamiento debería identificar las responsabilidades, los resultados esperados, el proceso de revisión a establecer, así como definir una política.³⁵

3.6 Análisis de impacto de negocio (BIA)

Una de las partes clave para desarrollar un plan de continuidad de servicios críticos de TI en una empresa constructora, es el BIA (Análisis de Impacto de Negocio) por sus siglas en inglés, ya que este análisis permite determinar principalmente el impacto operacional de los servicios como también el impacto económico.

El NIST brinda una plantilla general para poder desarrollar el BIA de un modo adecuado:

“El proceso BIA recomendado en esta guía está diseñado específicamente para utilizar las categorías y valores de impacto de identificación, determinar los objetivos de tiempo de recuperación (RTO) y priorizar los componentes del sistema para los sistemas de información. (...) El BIA en esta guía es un formato recomendado para sistemas de información; Las organizaciones pueden adaptar el formato a sus necesidades o utilizar un proceso diferente.” (NIST 2010: Appendix C-3)

El BIA se compone de los siguientes puntos:³⁶

- Determinar los procesos de negocio y su criticidad de recuperación. Se identifican los procesos de misión / negocio soportados por el sistema y se determina el impacto de una interrupción del sistema en esos procesos junto con los impactos de

³⁵ Cfr. Montero 2011: 23

³⁶ Cfr. NIST 800-34 B-1

interrupción y el tiempo de inactividad estimado. El tiempo de inactividad debe reflejar el máximo que una organización puede tolerar mientras mantiene la misión.

- Identificar los requerimientos de recursos. Los esfuerzos de recuperación realistas requieren una evaluación exhaustiva de los recursos necesarios para reanudar los procesos de negocios y las interdependencias relacionadas lo más rápido posible. Los ejemplos de recursos pueden ser: instalaciones, personal, equipos, software, archivos de datos, componentes del sistema y registros vitales.
- Identificar las prioridades de recuperación para los recursos del sistema. Sobre la base de los resultados de las actividades anteriores, los recursos del sistema se pueden vincular más claramente a los procesos críticos de negocio. Se pueden establecer niveles de prioridad para secuenciar actividades y recursos de recuperación.

El Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC) en el 2015 publicó una guía para la elaboración del BIA, en la cual muestra una matriz para evaluar la criticidad del servicio y su tolerancia a fallas de acuerdo a la función del negocio en el punto 5.1.3.2. Evaluación de Impactos Operacionales.³⁷

Tabla 2

Plantilla MINTIC

CATEGORÍA (FUNCIÓN DEL NEGOCIO)	PROCESO (SERVICIO)	NIVEL	TOLERANCIA A FALLAS (HORAS)	DESCRIPCIÓN
Aplicaciones	Sistema de Control de flujo de documentos	A	3	Contenedor de aplicaciones
	SQL nómina	B	1	Contenedor de aplicaciones en SQL

Fuente: MINTIC 2015

³⁷ Cfr. MINTIC 2015: 18

3.7 Estrategias de continuidad y alternativas de solución

Las estrategias de continuidad deben definir los enfoques para implementar la resiliencia requerida para que la detección, respuesta, recuperación y restauración de los servicios críticos de TI se pongan en marcha. La organización debe tener en cuenta la implementación y los requisitos de recursos en curso cuando está desarrollando la estrategia. Los proveedores externos pueden ser contratados para proporcionar servicios especializados y habilidades que juegan un papel importante en el apoyo a la estrategia.³⁸

En esta parte del plan, se debe evaluar una gama completa de alternativas de estrategia de continuidad y tienen que ser capaces de soportar los requisitos del negocio. Además, debe ser lo suficientemente flexible como para atender diferentes escenarios de paralización.

Las tecnologías que soportan los servicios críticos de TI generalmente requieren arreglos complejos para asegurar la continuidad, por lo que se debe tener en cuenta lo siguiente al seleccionar estrategias y alternativas de solución:³⁹

- a) RTO y RPO para servicios críticos de TI que apoyan las actividades críticas identificadas en el BIA.
- b) ubicación y distancia entre los sitios de TI;
- c) número de sitios de TI;
- d) acceso remoto a los sistemas;
- e) requisitos de climatización;
- f) requisitos de energía;
- g) el uso de sitios sin personal a diferencia de los sitios con personal;
- h) conectividad de telecomunicaciones y enrutamiento redundante;
- i) la naturaleza del "failback" (ya sea que se requiera intervención manual para activar la provisión alternativa de TI o si esto tiene que ocurrir automáticamente);
- j) nivel de automatización requerido;

³⁸ Cfr. ISO 27031 2011: 11

³⁹ Cfr. ISO 27031 2011: 12

k) obsolescencia tecnológica; y

l) la conectividad del proveedor de servicios subcontratados y otros enlaces externos.

3.8 Tiempos de recuperación y restauración (RTO y RPO)

La alta dirección de la empresa debe estar de acuerdo con la organización de los requisitos de continuidad de negocio. Estos requisitos darán lugar al Tiempo Objetivo de Recuperación (RTO) y al Punto Objetivo de Recuperación (RPO) para garantizar el Objetivo Mínimo de Continuidad del Negocio (MBCO) por servicio o actividad.⁴⁰

Estos tiempos empiezan desde el momento en que se produce la interrupción hasta la reanudación del servicio.

Puede haber varios servicios de Tecnología de la Información que se consideran críticos y necesarios para permitir la recuperación. Cada uno de estos servicios críticos de TI debe tener su propio y documentado Tiempo Objetivo de Recuperación y su Punto Objetivo de Recuperación. El RTO de los servicios críticos de TI será invariablemente menor que el RTO para la continuidad del negocio.

El Punto Objetivo de Recuperación se refiere a la cantidad de datos que se pierden y no son recuperables debido a la ruptura del servicio. Esto se representa en la cantidad de tiempo entre la última copia de seguridad buena y cuando se produce el evento de interrupción. El RPO varía en función de la estrategia de recuperación de servicios TIC empleado, particularmente en la disposición de copia de seguridad.⁴¹

Desde una perspectiva de continuidad de negocio existe un Tiempo Objetivo de Recuperación por servicio y que se inicia desde el punto en el que se produce la interrupción y se ejecuta hasta que el servicio se recupera, pero puede haber un número de servicios TIC necesarios para permitir esto y cada uno de estos servicios podrían comprender un número de sistemas o aplicaciones. Cada uno de ellos debe tener en cuenta la aceptación de los usuarios en el tiempo de prueba; a menos que el servicio de la continuidad del negocio pueda

⁴⁰ Cfr. ISO 27031 2011: 10

⁴¹ Cfr. ISO 27031 2011: 30

ser soportado sin TIC para un determinado período, por ejemplo, usando procedimientos manuales.⁴²

Figura 4. Hitos durante un proceso de interrupción

Fuente: Norma ISO 27031:2011

Además se debe equilibrar el costo de inoperabilidad de los sistemas contra el costo de los recursos necesarios para restaurar el sistema y su apoyo general a la misión crítica / procesos del negocio así como lo muestra la gráfica del NIST.

⁴² Cfr. ISO 27031 2011: 30

Figura 5. Balanceo de costos para los tiempos de recuperación

Fuente: Guía del NIST SP 800-34 Rev.1 2010

3.9 Política de continuidad

La organización en primer lugar debe definir una política de continuidad de servicios críticos de TI, donde pondrá los lineamientos generales para la aplicación del plan.

El NIST en su guía de implementación de plan de contingencia nos dice lo siguiente referente a la política de continuidad:

“El primer paso en el proceso de planificación de contingencia es desarrollar una declaración de política de planificación de contingencia con el apoyo de la alta dirección (normalmente el Director de Información). Esta política debe definir los objetivos generales de contingencia de la agencia y debe establecer el marco organizativo y responsabilidades para la planificación de contingencia sistema de información. La declaración de política también debe abordar las funciones y responsabilidades. La política debe ser apoyada con los procedimientos que cubren las necesidades de formación, la frecuencia de las copias de seguridad, los envíos de almacenamiento fuera del sitio, ejercicios de planes, pruebas y mantenimiento.”
(NIST 2010: Appendix C-2)

Es por eso que en el siguiente punto veremos los lineamientos que se definirán en la política de continuidad para la empresa JJC Contratistas Generales.

4 DEFINICIÓN DEL PROBLEMA

En base a la problemática descrita en el punto 2.3 (servicios lentos e inestables) se revisarán los puntos de análisis iniciales con información que ha sido recopilada de la organización objetivo como lo recomienda la norma ISO/IEC 27031:2011 y las demás guías vistas en el marco teórico para el desarrollo del plan.

Además se mostrará la EDT y una matriz de requerimientos asociada a todo el alcance y objetivos del proyecto.

4.1 Análisis de riesgos

4.1.1 Servicios críticos

Para el análisis de riesgos, primero se identificarán todos los servicios que brinda el área de Tecnología de la Información en la que se encuentra definidos los tres servicios críticos que se priorizarán para la continuidad del negocio.

A continuación en la Tabla 4 se muestra la lista general de servicios que brinda TI en la empresa JJC Contratistas Generales S.A. considerando la siguiente escala de valoración de la tabla 3:

Tabla 3
Escala de valoración de los servicios de TI

ESCALA	VALORACIÓN	DESCRIPCIÓN
1	Muy Alta	Servicio muy crítico que genera mucho valor al negocio y su interrupción genera mucha pérdida económica
2	Alta	Servicio crítico que podría generar mucho valor al negocio y su interrupción genera mucha pérdida económica
3	Media	Servicio no crítico que puede tolerar interrupciones pero que sí genera pérdida económica
4	Baja	Servicio no crítico que puede tolerar interrupciones y que genera poca pérdida económica
5	Muy Baja	Servicio no crítico que puede tolerar interrupciones y que no genera pérdida económica

Fuente: Elaboración propia

Esta valoración es definida por la propia organización junto con la Gerencia de TI para poder dar un nivel de criticidad a cada servicio de acuerdo a criterios internos que maneja la empresa para sus operaciones principales de negocio.

En la siguiente tabla, se pueden tener varios servicios críticos, pero para el diseño del plan sólo se consideran algunos: los definidos más críticos por la empresa y con valoración “Muy Alta”.

Los servicios con valoración 2 en adelante, como se indica en la tabla 4, *podrían o no* generar alguna pérdida para el negocio. Es por eso que sólo se considera los de valoración 1.

Tabla 4

Lista de servicios que brinda el área de TI de JJC Contratistas Generales

CÓDIGO	NOMBRE	DESCRIPCIÓN	VALORACIÓN
S-01	Active Directory	Servicio para la administración de políticas de acceso en toda la red de JJC.	2
S-02	Correo Móvil	Servicio de correo corporativo a través de dispositivo móvil.	3
S-03	Consola Antivirus	Servicio de Administración de Software de antivirus de usuarios de computadoras/laptops	2
S-04	Consola Spij	Aplicación para consulta del área legal.	4
S-05	Control de Acceso DC	Control biométrico para el acceso a DataCenter.	3
S-06	Control de Marcaciones de Asistencia	Servicio de marcación de registros de ingreso y salida de personal.	3
S-07	Correlacionador de eventos	Almacenamiento de registros de eventos de equipos de comunicaciones seguridad: switches y firewall.	5
S-08	Cuestionario (Eval. Personal Nuevo)	Servicio de cuestionario para test psicológicos de reclutamiento de personal.	3
S-09	Encuestas	Servicio de software de generación y envío de encuestas	5
S-10	Correo Electrónico	Servicio de correo corporativo	1

CÓDIGO	NOMBRE	DESCRIPCIÓN	VALORACIÓN
S-11	Factura Electrónica	Servicio de Facturación Electrónica	2
S-12	File Server	Servicio de almacenamiento y copias de seguridad de aplicaciones y archivos de usuarios de JJC.	1
S-13	GraphOn	Servicio acceso remoto a aplicaciones legacy	2
S-14	GraphOn Software	Servicio de acceso remoto a software especializado.	2
S-15	ISE Seguridad	Servicio de autenticación y autorización de acceso a la red.	2
S-16	JJC-SC File Server	Servicio de almacenamiento de archivos de usuarios de JJC-SC	2
S-17	JJC-SC SICO	Servicio de software de gestión de JJC-SC.	2
S-18	Legacy	Sistema de información legado de JJC.	2
S-19	Licencias de AutoCad	Servicio de administración de licencias de Autocad (usuarios en red)	2
S-20	Lync	Servicio de mensajería corporativa.	3
S-21	Mesa de Ayuda	Sistema de atención de incidencias y requerimientos a través de tickets.	2
S-22	Monitoreo de BI	Servicio para el monitoreo del sistema ERP de JJC.	3
S-23	Monitoreo Infraestructura	Monitoreo general de la infraestructura de red.	4
S-24	Monitoreo VCenter	Administración de plataforma de servidores centrales virtuales.	3
S-25	Radius - Postura	Servicio de control de acceso a la red.	3
S-26	OnBase	Servicio de Gestión de Contenido Empresarial de JJC.	2
S-27	PC para Conexión remota	Servicio de asistencia remota.	4
S-28	Project Server	Gestión de Proyectos.	3
S-29	S10 Presupuestos	Sistema de costos y presupuestos para Ingeniería.	2
S-30	SAP Dispatcher	Componente de acceso al sistema ERP vía Portal.	2
S-31	SAP Router	Componente de acceso al SAP BI e Infraestructura ERP.	2
S-32	SAP BI	Servicio para el monitoreo del sistema ERP de JJC.	2
S-33	Servicio de Impresoras	Servicio de Impresión en Red.	3

CÓDIGO	NOMBRE	DESCRIPCIÓN	VALORACIÓN
S-34	Servicio Web	Servicio de conexión Intranet e Internet.	3
S-35	SharePoint	Intranet corporativa.	2
S-36	SAP R3	Sistema de información de JJC.	1
S-37	Telefonía	Telefonía IP corporativa	3
S-38	Vmware Operation Manager	Monitoreo de servidores centrales	2
S-39	WSUS	Servicio de actualización de servicios Microsoft (Windows y Office)	4

Fuente: Elaboración propia con información de JJC Contratistas Generales

Como se observa en la tabla 4, a todos los servicios con valoración 1; es decir “muy alta”, se les considera los más importantes y críticos, dado que, en caso de ocurrir una paralización por algún incidente o evento, se debe priorizar cuáles serán los primeros en restablecerse para garantizar la continuidad del negocio.

4.1.2 Dimensiones de valoración

Para el análisis de riesgos se utilizará un dimensionamiento para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un servicio en una cierta dimensión es la medida del perjuicio para la organización si el servicio se ve dañado en dicha dimensión.

- a. **Disponibilidad [D]:** Propiedad o característica de los activos consistentes en que los usuarios o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- b. **Integridad [I]:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- c. **Confidencialidad [C]:** Propiedad o característica consistente en que la información no se pone a disposición, ni se revela a usuarios o procesos no autorizados.

- d. Autenticidad [A]:** Propiedad o característica consistente en que un usuario o entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- e. Trazabilidad [T]:** Propiedad o característica consistente en que las actuaciones de un usuario o entidad pueden ser imputadas exclusivamente a él.

4.1.3 Criterios de valoración

Estos criterios son las escalas cualitativas de valoración empleadas para la estimación del riesgo como lo recomienda la norma ISO/IEC 27031:2011 según el siguiente detalle:

a) Escala de Valoración de la Probabilidad:

Tabla 5

Escala de valoración de la probabilidad de ocurrencia de riesgos

ESCALA	PROBABILIDAD	DESCRIPCIÓN
MA	Muy Alta	Es muy probable que ocurra un evento de esta naturaleza en un periodo de tres meses.
A	Alta	Es probable que ocurra un evento de esta naturaleza en un periodo de 3 a 6 meses.
M	Media	El evento ocurrirá en algún momento en un periodo de 6 meses a un año.
B	Baja	Es poco probable que el evento suceda pero podría ocurrir en algún momento de un periodo de un año a dos años.
MB	Muy Baja	Es muy poco probable que el evento se presente en un periodo más de 2 años y no se detectaron vulnerabilidades que aumenten su probabilidad de ocurrencia.

Fuente: Elaboración propia

b) Escala de Valoración del Impacto:

De igual forma que la escala de valoración de probabilidad mostrada en la tabla 5, también se tiene una escala de valoración de impacto

Tabla 6
Escala de valoración del impacto

ESCALA	PROBABILIDAD	DESCRIPCIÓN
MA	Muy Alto	El evento provoca una interrupción completa de los servicios críticos de TI. Los procesos del negocio relacionados no tienen acceso a la infraestructura y tampoco a los recursos de información.
A	Alto	El evento provoca una interrupción entre parcial y completa de los servicios críticos de TI y afecta a todos los procesos relacionados.
M	Medio	El evento provoca una interrupción en los servicios de TI y esto afecta los procesos, pero las actividades críticas no son interrumpidas.
B	Bajo	El evento genera un leve impacto en los procesos, pero no ocasiona una interrupción importante en las operaciones. Afecta a menos de un 30% de los usuarios y dura lo suficiente para afectar levemente sus operaciones.
MB	Muy Bajo	El evento no provoca un impacto en los procesos. La interrupción de los servicios de TI afecta a uno o algunos usuarios, pero no dura lo suficiente para provocar un impacto en sus procesos.

Fuente: Elaboración propia

c) Escala de Valoración del Riesgo:

Tabla 7
Valoración del riesgo

ESCALA	RIESGO	DESCRIPCIÓN
MA	Crítico	Riesgo con mucha probabilidad de ocurrencia y con un alto impacto en la organización
A	Importante	Riesgo con probabilidad de ocurrencia media y con un alto impacto en la organización
M	Apreciable	Riesgo con probabilidad de ocurrencia y con un impacto considerable en la organización
B	Bajo	Riesgo con poca probabilidad de ocurrencia y con poco impacto en la organización.
MB	Despreciable	Riesgo con muy poca probabilidad de ocurrencia y con muy poco impacto en la organización

Fuente: Elaboración propia

Más adelante, en la evaluación del riesgo de cada escenario de amenaza se cruzarán los valores de las escalas de valoración de probabilidad e impacto. Como resultado de estas dos, obtendremos el nivel de riesgo que se manejará para las amenazas detectadas.

4.2 Análisis de amenazas

En este punto se procede a determinar las amenazas que pueden afectar a los servicios de TI, detallando las dimensiones de valoración (definidas en el punto anterior) de los recursos a los cuales afecta.

El resultado de la campo “Servicios Críticos Afectados” es el que ayudará a detectar qué amenaza afecta más a los servicios y para ver qué acción se tomará en el diseño del plan de continuidad más adelante.

Además, la dimensión de valoración asignada se da en base al criterio y experiencia del equipo de TI que realiza el análisis de amenazas.

Tabla 8

Análisis de amenazas existentes para los servicios críticos de TI

TIPO DE AMENAZA	AMENAZA	DIMENSIONES DE VALORACIÓN					DESCRIPCIÓN DETALLADA	SERVICIOS CRÍTICOS AFECTADOS
		[D]	[I]	[C]	[A]	[T]		
DESASTRES NATURALES	Inundación	X					Incidente que se produce sin intervención humana que afecte los recursos del sistema.	Todos los servicios brindados por TI
	Terremoto	X					Incidente que se produce sin intervención humana que afecte los recursos del sistema.	Todos los servicios brindados por TI
DESASTRES INDUSTRIALES	Incendio	X					Posibilidad de que un incendio acabe con los recursos del sistema.	Todos los servicios brindados por TI
	Avería del sistema de climatización	X					Fallo del sistema de aire acondicionado	Todos los servicios brindados por TI
	Corte de suministro eléctrico	X					Interrupción de la alimentación eléctrica.	Todos los servicios brindados por TI
	Problemas con el sistema de UPS	X					Problemas con el almacenamiento de energía en baterías	Todos los servicios brindados por TI

TIPO DE AMENAZA	AMENAZA	DIMENSIONES DE VALORACIÓN					DESCRIPCIÓN DETALLADA	SERVICIOS CRÍTICOS AFECTADOS
		[D]	[I]	[C]	[A]	[T]		
	Fallo de servicios de comunicaciones	X					Cese de la capacidad de transmitir datos de un lugar a otro.	S-10, S-12, S-36
ERRORES Y FALLOS NO INTENCIONADOS	Errores de los usuarios	X	X	X			Equivocaciones de las personas que hacen uso de los servicios de TI.	S-10, S-12, S-36
	Errores del administrador	X	X	X			Equivocaciones de las personas con responsabilidades de instalación y operación.	S-01, S-05, S-18, S-25, S-10, S-12, S-36, S-38
	Fallo en las copias de seguridad	X	X	X			Problemas con el Hardware / Software que realiza el back-up y la mala ejecución del proceso.	S-10, S-12, S-36
	Alteración accidental de la información		X				Equivocaciones de las personas que hacen uso de los servicios de TI.	S-10, S-12, S-36
	Destrucción de la información	X					Equivocaciones de las personas que hacen uso de los servicios de TI.	S-10, S-12, S-36
	Caída del sistema por agotamiento de recursos	X					Carencia de recursos que provoca la caída del sistema cuando la carga de trabajo es desmesurada.	S-10, S-12, S-36
	Carencia de Alta Disponibilidad (HA)	X					Carencia de Alta Disponibilidad de servicios críticos de TI.	Todos los servicios brindados por TI
ATAQUES INTENCIONADOS	Abuso de privilegios de acceso	X	X	X			Un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia.	S-12, S-18, S-35, S-36
	Difusión de software dañino	X	X	X			Propagación intencionada de virus y software malicioso.	S-12
	Modificación deliberada de la información		X				Alteración intencional de la información.	S-12, S-18, S-35, S-36
	Divulgación de información			X			Un usuario viola las políticas de seguridad de la información.	S-10, S-12, S-35
	Ataques por ingeniería social	X	X	X			Un atacante consigue robar información de un usuario a través de un engaño de Ingeniería Social	S-10, S-12, S-18, S-35, S-36

Fuente: Elaboración propia con información de JJC Contratistas Generales

4.3 Análisis de vulnerabilidades

En la tabla 9 se procede a analizar las vulnerabilidades existentes que podrían llegar a concretar amenazas que afectarían a los servicios de TI.

Al igual que el punto anterior, es muy importante el análisis de vulnerabilidad ya que se su resultado en el campo “Capacidad de Respuesta” ayudará a determinar el nivel de continuidad que se le está brindando actualmente a los servicios ante diversos escenarios.

Sobre los escenarios que no se tenga capacidad de respuesta o que ésta sea regular, se deberá tomar acciones en el diseño del plan a desarrollar.

Tabla 9

Análisis de vulnerabilidades existentes de los servicios críticos de TI

TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	PROTECCIÓN	CAPACIDAD DE RESPUESTA (SI/NO/REGULAR)
DESASTRES NATURALES	Inundación	Ubicación física del Centro de Datos en un área susceptible de desastres naturales	¿Los Centros de Cómputo están alejados de playas o ríos?	SI
	Terremoto	Ubicación física del Centro de Datos en un área susceptible de desastres naturales	¿Los Centros de Cómputo están construido con estructura antisísmica?	SI
DESASTRES INDUSTRIALES	Incendio	Ausencia de un sistema de extinción de fuegos	¿Existe sistema contra incendios?	SI
		Ausencia de mantenimiento a los sistemas contra incendios	¿Se le da mantenimiento al sistema contra incendios?	SI
	Avería del sistema de climatización	Ausencia de mantenimiento del sistema de aire acondicionado	¿Se realiza mantenimiento periódico al sistema de aire acondicionado?	SI
		Mantenimiento inapropiado del servicio técnico	¿Cuenta con personal calificado para mantenimiento?	SI
	Corte de suministro eléctrico	Ausencia de mantenimiento	¿Se brinda mantenimiento periódico al sistema eléctrico?	SI
		Cableado inapropiado	¿Se instaló un sistema eléctrico confiable?	SI
		Suministro eléctrico inapropiado	¿Se instaló un suministro eléctrico confiable?	SI

TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	PROTECCIÓN	CAPACIDAD DE RESPUESTA (SI/NO/REGULAR)
	Problemas con el sistema de UPS	Mantenimiento inapropiado del servicio técnico	¿Cuenta con personal calificado para mantenimiento?	SI
		Ausencia de mantenimiento	¿Se brinda mantenimiento periódico al UPS?	SI
		Cableado inapropiado	¿Se instaló un sistema equipo confiable?	SI
		Mantenimiento inapropiado del servicio técnico	¿Cuenta con personal calificado para mantenimiento?	SI
	Fallo de servicios de comunicaciones	Ausencia de Mantenimiento	¿Se brinda mantenimiento periódico a los equipos de comunicaciones?	REGULAR
		Cableado inapropiado	¿Se instaló cableado estructurado certificado?	SI
		Proveedor de servicios de comunicaciones no confiable	¿El proveedor de comunicaciones cumple con los niveles de servicio establecidos?	SI
		Ancho de banda inapropiado	¿Se provisionó un adecuado ancho de banda para el uso de las comunicaciones?	SI
ERRORES Y FALLOS NO INTENCIONADOS	Errores de los usuarios	Supervisión a los usuarios que utilizan servicios brindados por TI	¿Existe monitoreo permanente a los usuarios que utilizan los servicios críticos de TI?	REGULAR
	Errores del administrador	Ausencia o suspensión parcial de los servicios brindados por TI	¿Existe monitoreo permanente de los servicios críticos de TI?	REGULAR
		Personal suficiente para resolver todos los problemas que se presenten	¿Existe el personal suficiente para atender las caídas totales de los servicios críticos de TI?	REGULAR
	Fallo en las copias de seguridad	Ausencia de Back-up	¿Existen políticas de back-up para proteger los datos, los sistemas y las comunicaciones?	SI
		Personal técnico inexperto y con falta de conocimiento en el proceso de copias de seguridad	¿Cuenta con personal calificado para los procesos de respaldo?	REGULAR

TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	PROTECCIÓN	CAPACIDAD DE RESPUESTA (SI/NO/REGULAR)
		Falta de documentación de los procesos de respaldo y copias de seguridad	¿Cuenta con los manuales técnicos de respaldo actualizados junto con la documentación diaria, semanal y mensual de los Back-up?	REGULAR
	Alteración accidental de la información	Ausencia de mecanismos de monitoreo de la información disponible para los usuarios	¿Existen mecanismos de monitoreo y cambios de la información?	SI
		Falta de concientización e información al usuario sobre el uso y tratamiento de la información	¿Se realizan campañas para concientización e información al usuario sobre el uso y tratamiento de la información?	NO
	Destrucción de la información	Ausencia de mecanismos de monitoreo de la información disponible para los usuarios	¿Existen mecanismos de monitoreo y cambios de la información?	SI
		Falta de concientización e información al usuario sobre el uso y tratamiento de la información	¿Se realizan campañas para concientización e información al usuario sobre el uso y tratamiento de la información?	NO
	Caída del sistema por agotamiento de recursos	Monitoreo de uso de recursos	¿Se tiene un sistema de alertas y monitoreo de uso de recursos para evitar saturaciones de espacio, memoria y procesamiento?	SI
	Carencia de Alta Disponibilidad (HA)	Ausencia de Alta Disponibilidad para los servicios críticos	¿Se tiene implementados servicios de Alta Disponibilidad (HA) para los servicios críticos?	NO
		Ausencia de un plan de recuperación de servicios	¿Existe un plan de recuperación de servicios?	NO
		Personal suficiente y capacitado	¿Existe el personal suficiente y capacitado para gestionar el plan de continuidad?	REGULAR
ATAQUES INTENCIONADOS	Abuso de privilegios de acceso	Definición de privilegios de acceso inadecuada	¿Existen políticas de definición para otorgar derechos de acceso a los sistemas?	SI
		Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autenticación para acceso a los sistemas?	SI

TIPO DE AMENAZA	AMENAZA	VULNERABILIDAD	PROTECCIÓN	CAPACIDAD DE RESPUESTA (SI/NO/REGULAR)
		Ausencia de política de seguridad	¿Existen políticas para otorgar derechos de acceso a los sistemas?	SI
	Difusión de software dañino	Políticas de firewall inadecuadas	¿Existen políticas de firewall que protejan la seguridad de la red de datos?	SI
		Educación inadecuada del personal en virus y malware	¿Cuenta con personal calificado en conocimiento de virus?	REGULAR
		Carencia de software de antivirus	¿Se cuenta con software antivirus?	SI
		Falta de concientización e información al usuario sobre temas virus y software malicioso	¿Se realizan campañas para concientización e información al usuario sobre temas de virus y software malicioso?	REGULAR
	Modificación deliberada de la información	Ausencia de mecanismos de monitoreo de la información disponible para los usuarios	¿Existen mecanismos de monitoreo y cambios de la información?	REGULAR
	Divulgación de información	Ausencia de controles del tráfico de información a los usuarios	¿Existen controles de monitoreo al tráfico de información de los usuarios?	REGULAR
	Ataques por ingeniería social	Ausencia de mecanismos de identificación y autenticación	¿Existen mecanismos de identificación y autenticación para acceso a los sistemas?	SI
		Falta de concientización e información al usuario sobre mecanismos de ataques por ingeniería social	¿Se realizan campañas para concientización e información al usuario sobre mecanismos de ataques por ingeniería social?	REGULAR

Fuente: Elaboración propia con información de JJC Contratistas Generales

4.4 Edt

Figura 6. EDT

Fuente: Elaboración propia

Se ha definido además en la tabla 10 a todos los interesados del proyecto del diseño del plan de continuidad de servicios críticos de TI.

Tabla 10
Matriz de interesados

NOMBRE DEL INTERESADO	ORGANIZACIÓN A QUE PERTENECE	CATEGORÍA DE INTERESADO	NIVEL INTERÉS (BAJO, MEDIO, ALTO)	NIVEL INFLUENCIA (BAJO, MEDIO, ALTO)
Gerente Corporativo de Administración y Finanzas	JJC Contratistas Generales S.A.	Patrocinador	Alto	Alto
Todos las áreas de la empresa	JJC Contratistas Generales S.A.	Cliente	Medio	Bajo
Todos los usuarios de la empresa	JJC Contratistas Generales S.A.	Usuario	Medio	Bajo
Miembros del Directorio (Dueños de la empresa y Gerentes Corporativos)	JJC Contratistas Generales S.A.	Alta Dirección	Medio	Alto
Gerente de Tecnologías de la Información	JJC Contratistas Generales S.A.	Director Proyecto	Alto	Medio
Jefe de Servicios Tecnológicos	JJC Contratistas Generales S.A.	Miembro Proyecto	Alto	Medio
Administrador de Red	JJC Contratistas Generales S.A.	Miembro Proyecto	Alto	Bajo
Equipo Técnico de Redes	JJC Contratistas Generales S.A.	Miembro Proyecto	Medio	Bajo

Fuente: Elaboración propia con información de JJC Contratistas Generales

4.5 Alcance de la solución

El alcance de este diseño del plan de continuidad es para la Gerencia de Tecnología de la Información de la empresa JJC Contratistas Generales S.A. en su Data Center principal y secundario ya que es el área responsable de velar por la integridad, disponibilidad y confidencialidad de la información; para este caso específico, la continuidad de los tres servicios críticos que considera la organización.

En la siguiente tabla se muestran los requerimientos necesarios en cruce con los objetivos específicos para el desarrollo del diseño del plan de continuidad:

Tabla 11

Requerimientos para el desarrollo del plan de continuidad de servicios

RESUMEN DE OBJETIVOS ESPECÍFICOS Y REQUERIMIENTOS		
OBJETIVO ESPECÍFICO	REQUERIMIENTOS	
a. Identificar los riesgos de continuidad que podrían afectar los servicios críticos del área de Tecnología de la Información / <i>Control 6.3.2 de la norma ISO/IEC 27031:2011</i>	Análisis de Riesgos / Punto 6.3.3 norma ISO, Entendiendo los servicios críticos	*Se debe realizar el análisis de riesgos de todos los servicios brindados por TI. *Evaluar y entender los riesgos para darles el mejor tratamiento considerando todos los detalles que esto involucra.
	Análisis de Amenazas / Punto 6.3.3 norma ISO, Entendiendo los servicios críticos	*Se debe realizar el análisis de las amenazas que pueden afectar los servicios de TI con dimensiones de valoración ante diversos tipos de amenazas. *Considerar desastres naturales, desastres industriales, ataques intencionados, etc.
	Análisis de Vulnerabilidades / Punto 6.3.3 norma ISO, Entendiendo los servicios críticos	*Se debe realizar el análisis de vulnerabilidades existentes en el entorno y que podrían llegar a concretar amenazas que afectarían a los servicios de TI. *Considerar si se tiene una capacidad de respuesta ante las vulnerabilidades encontradas.
	Evaluación de Riesgos / Punto 6.3.3 norma ISO, Entendiendo los servicios críticos	*Con los tres análisis realizados antes, se debe hacer la evaluación de riesgos. *Evaluar la probabilidad de ocurrencia con el impacto y determinar el nivel de riesgo.
b. Desarrollar el análisis de impacto de negocio para poder determinar los impactos operacionales e impacto económico referente a los servicios críticos / <i>Anexo B del NIST SP 800-34 Rev. 1</i>	Business Impact Analysis (BIA) / Lineamientos descritos en el anexo B de la guía NIST para desarrollo del BIA	*Se debe desarrollar el BIA, necesario para ver los impactos operacionales e impactos económicos en el negocio en el caso de tener paralizaciones de los servicios. *Determinar los servicios de negocio y su criticidad. *Ver las prioridades de recuperación de servicios. *Identificar los recursos necesarios para el plan.
c. Establecer estrategias de recuperación y restauración de los servicios críticos del área de TI / <i>Control 6.4.2 de la norma ISO/IEC 27031:2011</i>	Escenarios de Amenazas y estrategias de continuidad / Punto 6.4.2 de la norma, Opciones de estrategias	*Se debe mostrar los diferentes escenarios de paralización de servicios críticos junto con sus diversas alternativas y de solución para poder definir estrategias de continuidad. *Las alternativas de continuidad tienen que ser capaces de soportar los requisitos del negocio y ser flexibles para actuar sobre diferentes escenarios de paralización.
d. Determinar periodos de recuperación requeridos por la organización para la continuidad de los servicios críticos del área de TI / <i>Control 6.4.2.4 y 7.4 de la norma ISO/IEC 27031:2011</i>	Diseño del plan de continuidad / Punto 6.4.2.4 y 7.4 de la norma, Datos y Operación	*Se debe mostrar las actividades del equipo de TI en el antes, durante y después de la interrupción de servicios críticos *Mostrar detalle de estrategias de continuidad y alternativas de solución en diversos escenarios. *Realizar los lineamientos generales de procedimientos y plantillas de continuidad.
	Prueba y validación de resultados / Punto 8.1.3 de la norma, Pruebas y ejercicios	*Realizar ejercicios y pruebas sobre algunos escenarios de paralización. *Validar resultados para demostrar mejora en tiempos de recuperación.

Fuente: Elaboración propia

5 DISEÑO DE LA SOLUCIÓN

En este punto se diseñará la política general de continuidad de negocio, así como los esquemas de responsabilidades de las personas que formarán los equipos de recuperación de servicios críticos, así como también se diseñarán los lineamientos generales de procedimientos iniciales para la elaboración del plan.

Además, se realizará la evaluación de riesgo junto con el análisis de impacto de negocio para poder detallar las estrategias y desarrollar las actividades de las alternativas de continuidad elegidas para cada escenario de amenaza definido.

5.1 Política de continuidad de negocio

La empresa JJC Contratistas Generales S.A. se encuentra comprometida en el desarrollo de un plan de continuidad de aquellos servicios de TI que son considerados críticos y que son de vital importancia para los procesos core (principales) de negocio en el caso de que se presente una interrupción parcial o total causada por problemas y/o incidentes que afecten dichos servicios.

Para esta política, la organización define los siguientes puntos:

- La empresa se compromete a brindar apoyo para poder garantizar que todos los procesos críticos del negocio operen continuamente con calidad y confiabilidad, mediante la realización del diseño de un plan de continuidad de servicios críticos de TI.
- Garantizar la protección de la vida humana, del medio ambiente, de los activos de la empresa, y la continuidad de los servicios críticos para la operación del negocio.
- Identificar y mitigar los riesgos, utilizando alternativas de solución en base a estrategias de continuidad evaluadas en el diseño del plan.
- Incluir en la cultura organizacional el concepto de continuidad de servicios críticos para una mejor ejecución del plan.
- Priorizar la asignación de recursos humanos y financieros para asegurar el cumplimiento de la presente política y la ejecución del plan de continuidad de servicios de TI.
- Mejorar continuamente el plan en base a pruebas realizadas como también escenarios reales.

La organización debe asegurarse de que todo el personal al que se le asignarán responsabilidades para el plan de continuidad de servicios críticos de TI sea competente para realizar las tareas requeridas tanto en la parte de análisis, mantenimiento de los registros de educación, formación, habilidades, experiencia y calificaciones.

Tabla 12
Detalle del equipo de TI para la continuidad de servicios

EQUIPO DE TI PARA LA CONTINUIDAD DE SERVICIOS CRÍTICOS					
CARGO	NOMBRE	FUNCIÓN	TELÉFONO CELULAR	TELÉFONO CASA	DIRECCIÓN CASA
Gerente de Tecnología de la Información	Ángela Carrasco Burneo	Responsable del Gerencia de TI	99#####	01-#####	Av. &&&&&&&&&&
Jefe Senior de Servicios Tecnológicos	Fernando Boza Gonzalez	Responsable de Servicios Tecnológicos e Infraestructura	99#####	01-#####	Cl. &&&&&&&&&&
Administrador de Redes y Comunicaciones II	Reich Sánchez Torres	Responsable de Infraestructura y Redes	99#####	01-#####	Cl. &&&&&&&&&&
Administrador de Redes y Comunicaciones I	Alexander Blanco Panduro	Responsable de Seguridad Informática y Servidores	99#####	01-#####	Jr. &&&&&&&&&&
Administrador de Redes y Comunicaciones I	Renzo Correa Salazar	Responsable de Servidores y Back-up	99#####	01-#####	Av. &&&&&&&&&&
Jefe de Desarrollo de Sistemas y Base de Datos	Geo Baccarani Rosas	Responsable de Desarrollo de Aplicaciones y Base de Datos	99#####	01-#####	Av. &&&&&&&&&&
Jefe de Soporte Tecnológico	Elvis Porras Poma	Responsable de Soporte y Producción	99#####	01-#####	Jr. &&&&&&&&&&

Fuente: Elaboración propia con información de JJC Contratistas Generales

5.3 Evaluación de riesgo

Para poder realizar la evaluación de los riesgos, se ha utilizado la matriz de probabilidad e impacto referente a las amenazas y su probabilidad de ocurrencia. (**Ver Anexo 1**).

Los resultados que muestra la tabla 13 son fundamentales ya que donde se muestra un nivel de riesgo como muy alto, serán los escenarios donde se deben desarrollar las alternativas de solución que harán que se evite, mitigue, transfiera o también que se acepten determinados riesgos.

Tabla 13
Evaluación de riesgos

TIPO DE AMENAZA	AMENAZA	PROBABILIDAD DE OCURRENCIA	IMPACTO	RIESGO
DESASTRES NATURALES	Inundación	M	A	A
	Terremoto	M	A	A
DESASTRES INDUSTRIALES	Incendio	MB	A	M
	Avería del sistema de climatización	M	M	M
	Corte de suministro eléctrico	M	MA	MA
	Problemas con el sistema de UPS	M	MA	MA
	Fallo de servicios de comunicaciones	M	MA	MA
ERRORES Y FALLOS NO INTENCIONADOS	Errores de los usuarios	M	M	M
	Errores del administrador	M	A	A
	Fallo en las copias de seguridad	M	MA	MA
	Alteración accidental de la información	M	M	M
	Destrucción de la información	M	MA	MA
	Caída del sistema por agotamiento de recursos	M	MA	MA
	Carencia de Alta Disponibilidad (HA)	M	MA	MA

TIPO DE AMENAZA	AMENAZA	PROBABILIDAD DE OCURRENCIA	IMPACTO	RIESGO
ATAQUES INTENCIONADOS	Abuso de privilegios de acceso	B	M	M
	Difusión de software dañino	B	A	A
	Modificación deliberada de la información	B	MA	MA
	Divulgación de información	M	A	A
	Ataques por ingeniería social	B	MA	MA

Fuente: Elaboración propia con información de JJC Contratistas Generales

5.4 Análisis de impacto de negocio (BIA)

Para realizar el Análisis de Impacto de Negocio de la empresa JJC Contratistas Generales S.A. se identificará las funciones del negocio útiles para apoyar la misión y los objetivos de la organización.

Este punto tiene como resultado generar un listado de roles y procesos que sirven de análisis para el cumplimiento de los siguientes pasos del BIA.

5.4.1 Identificación de procesos críticos

En primer lugar, se procede a definir los niveles de criticidad de los servicios que brinda la Gerencia de Tecnología de la Información, la cual se utiliza la matriz de niveles de criticidad de servicio (tabla 14) de la guía para realizar el BIA del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

Tabla 14
Niveles de criticidad de servicio

VALOR	INTERPRETACIÓN DEL PROCESO CRÍTICO
A	Crítico para el negocio
B	No es crítico para el negocio
C	No es parte integral del negocio

Fuente: MINTIC 2015

Para esta valoración se toma como referencia los niveles ya definidos por la organización en el punto 4.1 Análisis de Riesgos – Servicios Críticos que se muestra desde la página 28 a la 30.

5.4.2 Evaluación de impactos operacionales

El MINTIC brinda una matriz de impactos operacionales donde se identifican las categorías o funciones del negocio en la cual tienen como procesos principales los servicios críticos brindados por el área de TI. A estos procesos se les define el nivel de criticidad y su tiempo tolerable a fallas.

Tabla 15
Evaluación de impactos operacionales para los servicios críticos de JJC

CATEGORÍA DEL SERVICIO	SERVICIO	NIVEL	TOLERANCIA A FALLAS (HORAS)	DESCRIPCIÓN
Aplicaciones	Sistema SAP	A	8	Sistema Principal de la empresa JJC Contratistas Generales S.A.
	Correo Electrónico	A	8	Servidor Exchange Server 2010 para Correo Electrónico
Web	Página Web	B	12	Web de JJC
	Share Point	B	12	Portal interno para compartir información entre áreas.

CATEGORÍA DEL SERVICIO	SERVICIO	NIVEL	TOLERANCIA A FALLAS (HORAS)	DESCRIPCIÓN
Base de Datos	Oracle	B	3	Base de Datos del Sistema SAP
	SQL Server	B	3	Base de Datos de otros sistemas utilizados en la empresa como SharePoint
Seguridad de la Información	Firewall Perimetral	B	10	Equipo que brinda seguridad perimetral
	ISE / Radius	B	12	Servicio de seguridad para los puntos de red.
Sistemas de Almacenamiento	Servidores de Archivos	A	8	Servidores para guardar / compartir información
	SAN / Storage	B	4	Almacenamiento de Servidores
Comunicaciones	Internet	B	5	Servicio para navegar en Internet
	RPVL (Claro)	B	5	Servicio de conexión entre sedes de JJC
	MPLS (Americatel)	B	5	Servicio de conexión entre sedes de JJC

Fuente: Elaboración propia en base a la Plantilla MINTIC 2015

Referente a los tiempos de tolerancia a fallas, de acuerdo a pruebas realizadas por la Gerencia de TI y por la experiencia del área, en la tabla 15 se muestra el tiempo que cada servicio puede seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema; por consiguiente, la tolerancia a fallas es muy importante en aquellos sistemas que deben funcionar todo el tiempo.⁴³

Como se observa también en la tabla, los tres servicios críticos tienen un tiempo de 8 horas (día laboral) tolerable a fallas ya que deben contar con alternativas y mecanismos que le brinden alta disponibilidad apenas se detecte una falla en el servicio y así evitar una paralización.

⁴³ Cfr. MINTIC 2015: 18

5.4.3 Establecimiento de tiempos de recuperación

En este punto, utilizaremos los tiempos de recuperación recomendados por la norma ISO/IEC 27031:2011 y otras guías para la elaboración del diseño del plan de continuidad de servicios críticos.

En la siguiente tabla se describen los conceptos de los tiempos de recuperación que son fundamentales para el entendimiento de los periodos de restauración, recuperación, inactividad, etc. ante la caída de algún servicio.

Tabla 16

Descripción de tiempos de recuperación

TIEMPO DE RECUPERACIÓN	DESCRIPCIÓN
RPO	Punto en el tiempo que puede tolerar un proceso de negocio referente a la pérdida de datos.
RTO	Periodo de tiempo para poder recuperar los niveles de servicio mínimos y/o recursos que han sufrido una interrupción.
MTD	Periodo máximo de tiempo de inactividad que puede tolerar la entidad sin entrar en colapso.

Fuente: ISO/IEC 27031:2011

La tabla 17 es una plantilla dada por MINTIC pero aplicada a los servicios de TI de JJC Contratistas Generales donde se muestra la prioridad de recuperación de cada servicio, pero sólo los tres servicios críticos están con prioridad “1”. Además se muestra el MTD (periodo máximo de inactividad) en horas para los servicios críticos. Esto viene a ser el tiempo máximo que la organización puede estar con el servicio paralizado.

Tabla 17
Prioridades de recuperación de servicios críticos

CATEGORÍA DEL SERVICIO	SERVICIO	MTD (HORAS)	PRIORIDAD DE RECUPERACIÓN
Aplicaciones	Sistema SAP	24	1
	Correo Electrónico	24	1
Web	Página Web	48	3
	Share Point	36	2
Base de Datos	Oracle	36	2
	SQL Server	36	2
Seguridad de la Información	Firewall Perimetral	28	2
	ISE / Radius	36	3
Sistemas de Almacenamiento	Servidores de Archivos	24	1
	SAN / Storage	28	2
Comunicaciones	Internet	32	2
	RPVL (Claro)	28	2
	MPLS (Americatel)	28	2

Fuente: Elaboración propia en base a la Plantilla MINTIC 2015

En la tabla 18, se define el punto y tiempo de recuperación. Es importante señalar la diferencia entre ambos, ya que punto de recuperación se refiere al tiempo soportado por la empresa en relación a la pérdida de datos, mientras que tiempo de recuperación se refiere al periodo donde se restablecerán los servicios mínimos para seguir operando.

Estos tiempos serán medidos más adelante para ser comparados con los tiempos de recuperación propuestos luego del diseño del plan de continuidad de servicios.

Tabla 18

Disposición de los RPO/RTO por cada servicio crítico

CATEGORÍA DEL SERVICIO	SERVICIO	IDENTIFICACIÓN DE RECURSOS CRÍTICOS	PUNTO DE RECUPERACIÓN OBJETIVO – RPO (HORAS)	TIEMPO DE RECUPERACIÓN OBJETIVO – RTO (HORAS)
Aplicaciones	Sistema SAP	* Enlace de contingencia para llegar al hosting / housing de IBM * Sistema de Back-up	20	24
	Correo Electrónico	* Sistema de replicación DFS (HA) * Sistema de Back-up	20	24
Web	Página Web	* Control de operaciones del servidor web	40	48
	Share Point	* Servidores de contingencia en Data Center Alterno * Sistema de Back-up	30	36
Base de Datos	Oracle	* Servidores de contingencia en Data Center Alterno * Sistema de Back-up	30	24
	SQL Server	* Servidores de contingencia en Data Center Alterno * Sistema de Back-up	30	24
Seguridad de la Información	Firewall Perimetral	* Equipo pasivo con la misma configuración * Back-up de configuraciones	25	36
	ISE / Radius	* Equipo pasivo con la misma configuración * Back-up de configuraciones	30	72
Sistemas de Almacenamiento	Servidores de Archivos	* Sistema de replicación DAG (HA) * Sistema de Back-up	20	24
	SAN / Storage	* Servidores replicados en el Data Center Alterno * Sistema Back-up	22	36
Comunicaciones	Internet	* Enlace de contingencia con otro proveedor para la salida a Internet * Routers con alta disponibilidad (HA)	22	36
	RPVL (Claro)	* Enlace de contingencia con otro proveedor para la RPVL * Routers con alta disponibilidad (HA)	25	36
	MPLS (Americatel)	* Enlace de contingencia con otro proveedor para la MPLS * Routers con alta disponibilidad (HA)	25	36

Fuente: Elaboración propia en base a la Plantilla MINTIC 2015

5.4.4 Impacto económico

Para poder evaluar el impacto económico debemos saber que el riesgo de cada componente está en función directa a las pérdidas que ocasionará que el servicio crítico de TI deje de operar o funcionar, así como de cuán vulnerable es dicho servicio en ese momento.

El riesgo no es fácil de cuantificar, siendo en general un estimador subjetivo; es por eso que la empresa JJC Contratistas Generales ha realizado una estimación para encontrar un monto para cada servicio. Para ello, nos basaremos en una fórmula básica que nos brinda en Diego Bravo Estrada en un artículo donde incluye recomendaciones sobre el análisis de riesgos y su estimación económica.⁴⁴

$$\textbf{RIESGO TOTAL} = \textbf{RIESGO (componente 1)} + \textbf{RIESGO (componente 2)} + \dots$$

$$\textbf{RIESGO (componente)} = P * V$$

A continuación se detalla la explicación de la fórmula:

“Donde P=pérdida, es la pérdida en dinero que implicaría la inoperatividad del componente hasta su reparación, aunque se pueden agregar otros estimadores como el desprestigio ante nuestros clientes. A veces ayuda considerarlo como "el valor" que representa para la organización. V=vulnerabilidad, es tanto o más subjetiva puesto que no hay una manera segura de establecer para todos los casos si los supuestos mecanismos de protección (del componente) son o no realmente confiables (...). Por ejemplo, se puede asignar números como 1, 2, 3, 4, para señalar una vulnerabilidad mínima, regular, importante y peligrosa, respectivamente.” (Bravo 2010:3)

⁴⁴ Cfr. Bravo 2010: 3

Con la fórmula de Bravo, en la tabla 19 se encuentra el monto de pérdida estimada inicial para cada servicio. **Este monto es un cálculo confidencial brindado por el área de TI.**

El resultado de este cálculo, servirá para obtener un monto más real del impacto económico de cada servicio que será mostrado en la tabla 20.

Tabla 19

Cálculo de pérdida económica estimada por hora de cada servicio de JJC

SERVICIO	ESTIMACIÓN CONFIDENCIAL DE PÉRDIDA	NIVEL DE VULNERABILIDAD ESTIMADA (SEGÚN CRITICIDAD)	PÉRDIDA ECONÓMICA ESTIMADA TOTAL X SERVICIO
Sistema SAP	S/ 401.79	3	S/ 1,205.38
Correo Electrónico	S/ 247.29	3	S/ 741.88
Página Web	S/ 80.00	1	S/ 80.00
Share Point	S/ 34.17	2	S/ 68.33
Oracle	S/ 43.75	2	S/ 87.50
SQL Server	S/ 63.33	2	S/ 126.67
Firewall Perimetral	S/ 45.83	2	S/ 91.67
ISE / Radius	S/ 18.75	1	S/ 18.75
Servidores de Archivos	S/ 331.25	3	S/ 993.75
SAN / Storage	S/ 64.58	2	S/ 129.17
Internet	S/ 47.92	2	S/ 95.83
RPVL (Claro)	S/ 40.25	2	S/ 80.50
MPLS (Americatel)	S/ 38.63	2	S/ 77.25

Fuente: Elaboración propia con información de JJC Contratistas Generales – Año 2017

Para el cálculo de impacto económico por cada servicio, la Gerencia de TI de la empresa JJC Contratistas Generales ha elaborado una fórmula sencilla en base a la experiencia y análisis de sus colaboradores:

Costo de paralización de un servicio X día = (Pérdida fija del servicio) X (nro. de horas de caída del servicio) + (*Costo de detección del problema y la restauración del servicio)

Fuente: JJC Contratistas Generales

NOTA: * en caso se llame a un proveedor o todo lo relacionado a la detección de problema.

Tabla 20

Estimación de impacto económico por día para los servicios críticos de JJC

SERVICIO	PÉRDIDA FIJA X SERVICIO	HORAS DE CAÍDA	COSTO DE DETECCIÓN DE PROBLEMA Y RESTAURACIÓN DEL SERVICIO	TOTAL PÉRDIDA X DÍA
Sistema SAP	S/ 1,205.38	24	S/ 550.00	S/ 29,479.00
Correo Electrónico	S/ 741.88	24	S/ 350.00	S/ 18,155.00
Página Web	S/ 80.00	24	S/ 250.00	S/ 2,170.00
Share Point	S/ 68.33	24	S/ 250.00	S/ 1,890.00
Oracle	S/ 87.50	24	S/ 250.00	S/ 2,350.00
SQL Server	S/ 126.67	24	S/ 250.00	S/ 3,290.00
Firewall Perimetral	S/ 91.67	24	S/ 250.00	S/ 2,450.00
ISE / Radius	S/ 18.75	24	S/ 250.00	S/ 700.00
Servidores de Archivos	S/ 993.75	24	S/ 350.00	S/ 24,200.00
SAN / Storage	S/ 129.17	24	S/ 250.00	S/ 3,350.00
Internet	S/ 95.83	24	S/ 250.00	S/ 2,550.00
RPVL (Claro)	S/ 80.50	24	S/ 250.00	S/ 2,182.00
MPLS (Americatel)	S/ 77.25	24	S/ 250.00	S/ 2,104.00
TOTAL				S/ 94,870.00

Fuente: Elaboración propia con información de JJC Contratistas Generales – Año 2017

En el caso de que el sistema SAP se paralice por un día, considerando que dichas horas sean luego del tiempo tolerable por la organización, la pérdida de dinero se estima en **S/ 29,479.00**. Del mismo modo, si se detiene el servicio de correo electrónico, la pérdida

estimada sería de **S/. 18,155.00**. Por último, si se detiene el servicio de los servidores de archivos, la pérdida sería de **S/. 24,200.00** aproximadamente.

En total la detención de **sólo** los servicios críticos de TI costaría **S/. 71,834.00**; este valor incrementa dado que se considera las vulnerabilidades junto con el nivel de criticidad del servicio.

En la tabla 20 observamos que en caso de no tener operativos los servicios de TI en la organización, el impacto económico total de pérdida para la empresa sería aproximadamente **S/. 94,870.00** por un día paralizado, teniendo en cuenta que la cifra puede variar dependiendo del tiempo de paralización y de los medios utilizados para el restablecimiento de los servicios.

5.5 Estrategias de continuidad

Para plantear las estrategias de continuidad, nos basaremos en las amenazas identificadas con un riesgo considerado como “Muy Alto” para poder proponer alternativas de solución que se adecuen a posibles escenarios de interrupción.

Se brindará el detalle de cómo se actuará ante cada posible escenario de paralización con diferentes causas. Si bien es cierto, se plantean diversos escenarios, pero en esta matriz se hace **énfasis** en los tres servicios críticos principales considerados por la organización objetivo (Sistema SAP, Correo Electrónico y Servidores de Archivos).

Las estrategias para el plan de continuidad de servicios críticos de TI se muestran a continuación en la tabla Nro. 21:

Tabla 21
Estrategias de continuidad

TIPO DE AMENAZA	AMENAZA	RIESGO	ITEM	POSIBLE ESCENARIO DE FALLA DE LOS SERVICIOS	POSIBLE CAUSA DE FALLA DE LOS SERVICIOS	NRO DE ESTRATEGIA	ESTRATEGIA(S) DE CONTINUIDAD
DESASTRES INDUSTRIALES	Corte de suministro eléctrico	MA	1	Corte de suministro eléctrico por parte de Luz del Sur en la oficina principal	Problema de alguna central del proveedor en la zona donde se ubica la oficina principal	1	* Contar con un sistema óptimo de UPS * Contar con un grupo electrógeno estable en el edificio * Tener un procedimiento definido para establecer un contacto inmediato con el proveedor de energía eléctrica
			2	Problema en los equipos de los tableros de energía eléctrica dentro de la oficina principal	Falla de alguna llave o falla de cables que genere el corte de energía en el edificio	2	* Contar con un sistema óptimo de UPS * Contar con un grupo electrógeno estable en el edificio * Tener un procedimiento definido para establecer un contacto inmediato con el proveedor de energía eléctrica
	Problemas con el sistema de UPS	MA	3	Problema de un UPS que alimente un gabinete principal que aloje servidores críticos	Fallo general de las baterías de dicho UPS que no pueda soportar la carga de servidores críticos	3	* Contar con un grupo electrógeno estable en el edificio con sistemas bypass
			4	Corte de energía al realizar un mantenimiento preventivo	Fallo de la configuración ByPass para realizar los mantenimientos preventivos	4	* Contar con un grupo electrógeno estable en el edificio con sistemas bypass * Tener un procedimiento definido para establecer un contacto inmediato con el proveedor de energía eléctrica y con el ingeniero eléctrico del edificio
	<u>Fallo de servicios de comunicaciones</u>	MA	5	Fallo en el servicio RPVL (Claro)	Problema con el router ubicado en la oficina principal	5	* Contar con un proveedor alternativo para que entre en funcionamiento inmediatamente luego de una caída
					Problema con la red del proveedor	6	* Contar con un proveedor alternativo para que entre en funcionamiento inmediatamente luego de una caída

TIPO DE AMENAZA	AMENAZA	RIESGO	ITEM	POSIBLE ESCENARIO DE FALLA DE LOS SERVICIOS	POSIBLE CAUSA DE FALLA DE LOS SERVICIOS	NRO DE ESTRATEGIA	ESTRATEGIA(S) DE CONTINUIDAD
			6	Corte del servicio de Internet (Claro)	Falta de pago del servicio	7	* Comunicar inmediatamente al área de pagos de facturas * Contar con un proveedor alternativo para que entre en funcionamiento inmediatamente luego de una caída
					Problema con el router ubicado en la oficina principal	8	* Contar con un proveedor alternativo para que entre en funcionamiento inmediatamente luego de una caída
					Problema con la red del proveedor	9	* Contar con un proveedor alternativo para que entre en funcionamiento inmediatamente luego de una caída
			7	<u>Corte del Sistema SAP</u>	Caída por error de programación de mismo sistema SAP	10	* Contactar inmediatamente al proveedor IBM para la revisión del servicio
					Problema con el router ubicado en la sede del proveedor que brinda el Hosting y Housing	11	* Contar con un proveedor alternativo para que entre en funcionamiento inmediatamente luego de una caída
ERRORES Y FALLOS NO INTENCIONADOS	<u>Fallo en las copias de seguridad</u>	MA	8	<u>Problema de Hardware / Software del sistema de copias de seguridad</u>	Mala realización de la copia de seguridad (no se realizó prueba de restauración periódica)	12	* Tener un sistema de replicación en el Data Center de alternativo (Villa el Salvador) para proceder a recuperar la información * Buscar y restaurar una copia de información con más anterioridad que la esperada a la fecha de pérdida
					Mal cálculo de espacio en cinta para back-up	13	* Tener un sistema de replicación en el Data Center de alternativo (Villa el Salvador) para proceder a recuperar la información * Buscar y restaurar una copia de información con más anterioridad que la esperada a la fecha de pérdida

TIPO DE AMENAZA	AMENAZA	RIESGO	ITEM	POSIBLE ESCENARIO DE FALLA DE LOS SERVICIOS	POSIBLE CAUSA DE FALLA DE LOS SERVICIOS	NRO DE ESTRATEGIA	ESTRATEGIA(S) DE CONTINUIDAD
					Problema de cinta malograda	13	* Tener un sistema de replicación en el Data Center de alerno (Villa el Salvador) para proceder a recuperar la información * Buscar y restaurar una copia de información con más anterioridad que la esperada a la fecha de pérdida
	<u>Dstrucción de la información</u>	MA	9	<u>Borrado de información en algún servicio utilizado por el usuario final</u>	Mal tratamiento de los archivos	14	* Tener un sistema de replicación en el Data Center de alerno (Villa el Salvador) para proceder a recuperar la información * Buscar y restaurar una copia de información con más anterioridad que la esperada a la fecha de pérdida
					No bloquear las sesiones utilizadas para los diversos servicios	14	* Tener un sistema de replicación en el Data Center de alerno (Villa el Salvador) para proceder a recuperar la información * Buscar y restaurar una copia de información con más anterioridad que la esperada a la fecha de pérdida
			10	Incidente ocurrido al proveedor custodio en el traslado de copias de seguridad	Poca seguridad utilizada para trasladar las copias de la información	15	* Tener un sistema de replicación en el Data Center de alerno (Villa el Salvador) para proceder a recuperar la información * Buscar y restaurar una copia de información con más anterioridad que la esperada a la fecha de pérdida
	<u>Caída del sistema por agotamiento de recursos</u>	MA	11	Saturación de procesamiento, memoria y espacio en servidores	Mala configuración de balanceo de carga entre servidores	16	* Solicitar apoyo urgente al proveedor Corporación Sapia (según los SLA) para reconfigurar un balanceo de carga entre servidores críticos * Detener procesos no críticos para poder

TIPO DE AMENAZA	AMENAZA	RIESGO	ITEM	POSIBLE ESCENARIO DE FALLA DE LOS SERVICIOS	POSIBLE CAUSA DE FALLA DE LOS SERVICIOS	NRO DE ESTRATEGIA	ESTRATEGIA(S) DE CONTINUIDAD
							liberar espacio, memoria, etc. necesarios para mejorar el rendimiento
					No hay configuración de alertas en los equipos de monitoreo	17	* Solicitar apoyo urgente al proveedor Corporación Sapia (según los SLA) para reconfigurar un balanceo de carga entre servidores críticos * Detener procesos no críticos para poder liberar espacio, memoria, etc. necesarios para mejorar el rendimiento
					Falta de monitoreo por parte del administrador de red	18	* Solicitar apoyo urgente al proveedor Corporación Sapia (según los SLA) para reconfigurar un balanceo de carga entre servidores críticos * Detener procesos no críticos para poder liberar espacio, memoria, etc. necesarios para mejorar el rendimiento
	<u>Carencia de Alta Disponibilidad (HA)</u>	MA	12	<u>Problema de réplicas entre servidores de archivos</u>	Mala configuración de las réplicas del servicio DFS	19	* Solicitar apoyo urgente al proveedor Corporación Sapia (según los SLA) para revisar configuración de réplicas * Buscar y restaurar la copia de información más cercana a la fecha de la última replicación
			13	<u>Problema de réplicas del servidor de correo</u>	Mala configuración del servicio DAG para replicación de bases de datos	20	* Solicitar apoyo urgente al proveedor Corporación Sapia (según los SLA) para revisar configuración de réplicas * Buscar y restaurar la copia de información más cercana a la fecha de la última replicación

TIPO DE AMENAZA	AMENAZA	RIESGO	ITEM	POSIBLE ESCENARIO DE FALLA DE LOS SERVICIOS	POSIBLE CAUSA DE FALLA DE LOS SERVICIOS	NRO DE ESTRATEGIA	ESTRATEGIA(S) DE CONTINUIDAD
ATAQUES INTENCIONADOS	Modificación deliberada de la información	MA	14	Borrado de archivos importantes de otra área o usuario	Usuario disconforme / molesto / etc.	21	* Tener un sistema de replicación en el Data Center de alerno (Villa el Salvador) para proceder a recuperar la información * Buscar y restaurar una copia de información con más anterioridad que la esperada a la fecha de pérdida
			15	Daño de archivos de algún sistema crítico	Usuario disconforme / molesto / etc.	22	* Recuperar un servidor físico / virtual necesario para levantar el sistema / aplicación que fue dañada * Buscar y restaurar la copia de información más cercana a la fecha de pérdida
	Ataques por ingeniería social	MA	16	Ingreso de un atacante a los servicios para borrar y/o robar información de la empresa	Usuario que brinda credenciales de acceso o información confidencial que le sirve al atacante para ingresar a los servicios	23	* Revisar logs de accesos para identificar y cerrar puertos y conexiones utilizadas por el atacante * Cerrar conexiones a los sistemas * Realizar copias de seguridad de la información y enviarlas urgente al proveedor custodio

Fuente: Elaboración propia con información de JJC Contratistas Generales

5.6 Actividades del equipo de TI en el antes, durante y después de la interrupción de servicios críticos

Así como en las guías de diseño de plan de continuidad de servicios, Marco Ochoa en su tesis plantea las actividades del equipo de TI las cuales se han tomado como base para aplicarlo y mejorarlo en la empresa JJC Contratistas Generales. Esto se muestra a continuación:

a) Actividades del plan que se deben realizar antes de una interrupción de servicio(s) crítico(s) de TI ⁴⁵

Antes de que se presente alguna interrupción de servicio por determinada causa, el equipo de TI para la continuidad debe asegurarse que todos los registros deben estar completos y disponibles tanto dentro de la organización como fuera de ésta; es decir, que se debe tener evidencia de los siguientes puntos:

- Que se encuentre elaborado y probado cada procedimiento que se aplicará en cada emergencia para restablecer el servicio de TI, así como también, cada procedimiento que se utilizará para continuar las operaciones del día a día, hasta que se restablezca el servicio. Esto incluye la capacitación, entrenamiento, seguimiento, evaluación y acciones sub-siguientes.
- Que se encuentre elaborada la lista del personal interno y externo a quien se reportará determinado incidente.
 - El personal debe estar capacitado, entrenado, comprometido y motivado para desarrollar las actividades que cada emergencia exige.
 - Debe estar todo el personal de emergencias presente cuando sean llamados y deberán trabajar en el horario y por el tiempo que sea necesario hasta lograr restablecer la prestación del servicio interrumpido.
- Asegurarse que se encuentren disponibles cada uno de los recursos que sean indispensables para mantener la continuidad de las operaciones de la organización.
- Que se encuentren guardados los registros, incluidos las guías de instalación, configuraciones, usuarios, roles, accesos, niveles de privilegios, etc., y que sean almacenados tanto dentro como fuera de la organización.

⁴⁵ Cfr. Ochoa 2015: 139

- Que este actualizado y probado el plan de continuidad de los servicios críticos de TI, incluidas las lecciones aprendidas de la última emergencia superada.
- Una vez realizadas las pruebas pertinentes para comprobar que el plan ha funcionado tal y como se esperaba; hay que evaluarlo para retroalimentar con comentarios, conclusiones y recomendaciones que permitan mejorarlo, ajustándolo a las nuevas necesidades. Las pruebas a realizar son pruebas de: seguridad, mantenimiento, soporte, recuperación, disponibilidad, funcionalidad y desempeño.

b) Actividades del plan que se deben realizar durante una interrupción de servicio(s) crítico(s) de TI ⁴⁶

Cuando se presenta alguna interrupción de servicio por determinada causa, el equipo de TI para la continuidad debe asegurarse que todos los registros debe estar completos y disponibles tanto dentro de la organización como fuera de ésta; es decir, que se debe realizar los siguientes puntos:

- Una vez establecida la emergencia e informada a los responsables de cada uno de los servicios críticos de TI, se debe convocar al personal del equipo de TI responsable.
- Que se utilicen los registros del plan, incluidos todos los recursos indispensables para la recuperación en la misma organización o en el Data Center alternativo.
- Que se ponga en práctica la capacitación y entrenamiento de todos los miembros del equipo de TI para la continuidad en los roles y actividades a realizar para que tengan las capacidades necesarias para restablecer el servicio, utilizando los procedimientos establecidos en las listas de chequeo del plan.
- Que se encuentre establecido, actualizado y probado el plan de continuidad de los servicios críticos de TI, incluidas las lecciones aprendidas de la última emergencia superada.
- Que las copias de seguridad estén disponibles para realizar la recuperación de datos y/o aplicaciones de acuerdo al caso.
- Que se ejecute el procesamiento en el Data Center alternativo en caso sea necesario durante el periodo de emergencia.

⁴⁶ Cfr. Ochoa 2015: 141

c) Actividades del plan que se deben realizar después de una interrupción de servicio(s) crítico(s) de TI ⁴⁷

Se debe verificar que se hayan cumplido todas las actividades y procedimientos que fueron necesarios para superar la emergencia; documentar todo lo nuevo referente a estos procedimientos y documentos que se deban emplear en nuevas emergencia; es decir, que se debe tener evidencia de los siguientes puntos:

- Que esté establecido, actualizado y probado el plan de continuidad de los servicios críticos de TI, incluidas las lecciones aprendidas de la última emergencia superada.
- Validar y asegurar antes del restablecimiento de los servicios brindados lo siguiente:
 - La confiabilidad de la documentación en la cual tiene guardado los últimos registros procesados antes de declararse la emergencia.
 - La certeza de que la información registrada antes de la emergencia sean los correctos.
 - Asegurarse que se hayan ingresado todos los registros realizadas durante el periodo de emergencia, si falta alguno, establecer los pasos para procesarla y recuperarla.
 - Que la información esté documentada y respaldada en los escenarios antes, durante y después de la emergencia, con la respectiva evaluación que permita retroalimentar con comentarios, conclusiones y recomendaciones para mejorar el plan, ajustándolo a las nuevas necesidades.
- Se debe declarar el cierre de la emergencia por parte de los responsables de los servicios críticos de TI restablecidos.
- Se debe firmar las actas del retorno a la normalidad.
- Presentar el reporte final de la emergencia superada y que debe incluir lo siguiente:
 - El diagnóstico de las causas raíz que ocasionaron la interrupción del servicio crítico de TI.
 - Lo relevante de la recuperación, las estrategias aplicadas los resultados obtenidos y un breve resumen del trabajo realizado.

⁴⁷ Cfr. Ochoa 2015: 144

- El retorno a la normalidad con los comentarios conclusiones y recomendaciones que permitan el mejoramiento del plan mediante las lecciones aprendidas en cada emergencia superada.
- La vigencia de este plan empezará desde el día de su comunicación.

5.7 Lineamientos generales para las alternativas de solución en los diversos escenarios

A continuación se detallará las acciones y actividades de las alternativas de continuidad frente a distintos escenarios de paralización o interrupción de los servicio críticos de TI.

1) Corte de suministro eléctrico por parte del proveedor Luz del Sur en la oficina principal

Acciones a seguir si ocurre un problema de alguna central del proveedor en la zona donde se ubica la oficina principal:

- a. Comunicar inmediatamente al proveedor de energía eléctrica.
- b. Asegurar que los UPS entren en funcionamiento y alertar a los responsables del plan de continuidad de servicios críticos de TI.
- c. Asegurar la operatividad del grupo electrógeno del edificio junto con el área Logística.

En paralelo se deben realizar las siguientes actividades:

1. Realizar junto con el área Logística el seguimiento urgente al proveedor de energía eléctrica para restablecer el servicio.
2. Validar la continuidad del funcionamiento del UPS del Data Center.
3. Validar la operatividad del funcionamiento del grupo electrógeno del edificio.
4. Asegurar la conectividad / operatividad con el Data Center alternativo en Villa el Salvador en caso requiera entrar en acción.

2) Problema en los equipos de los tableros de energía eléctrica dentro de la oficina principal

Acciones si ocurre la falla de alguna llave eléctrica o falla de cables que genere el corte de energía en el edificio:

- a. Comunicar inmediatamente a los ingenieros eléctricos del edificio y al proveedor de energía eléctrica.
- b. Asegurar que los UPS del Data Center entren en funcionamiento y alertar a los responsables del plan de continuidad de servicios críticos de TI.
- c. Asegurar la operatividad del grupo electrógeno del edificio.

En paralelo se deben realizar las siguientes actividades:

1. Realizar seguimiento urgente a los ingenieros eléctricos del edificio y al proveedor de energía eléctrica para restablecer el servicio.
2. Validar la continuidad de funcionamiento de UPS.
3. Validar la operatividad de funcionamiento del grupo electrógeno del edificio.

3) Problema de un UPS que alimente un gabinete principal que aloje servidores críticos

Acciones si ocurre algún fallo general de las baterías de algún UPS que no pueda soportar la carga de servidores críticos:

- a. Comunicar inmediatamente al proveedor de UPS.
- b. Alertar a los ingenieros eléctricos del edificio para monitorear la estabilidad del servicio de energía.
- c. Asegurar que el grupo electrógeno entre en funcionamiento y alertar a los responsables del plan de continuidad de servicios críticos de TI.

En paralelo se deben realizar las siguientes actividades:

1. Realizar seguimiento urgente al proveedor de UPS para ponerlo operativo nuevamente.
2. Validar la continuidad de funcionamiento del grupo electrógeno del edificio.
3. Revisar la conectividad / operatividad con el Data Center alternativo en Villa el Salvador en caso requiera entrar en acción.

4) Corte de energía al realizar un mantenimiento preventivo

Acciones si ocurre algún fallo de la configuración ByPass para realizar los mantenimientos preventivos:

- a. Asegurar que inmediatamente el proveedor de UPS brinde una solución lo más pronto posible.
- b. Alertar a los ingenieros eléctricos del edificio para monitorear la estabilidad del servicio de energía y asegurar que los otros UPS entren en funcionamiento.
- c. Asegurar que el grupo electrógeno entre en funcionamiento y alertar a los responsables del plan de continuidad de servicios críticos de TI.

En paralelo se deben realizar las siguientes actividades:

1. Realizar seguimiento urgente al proveedor de UPS para ponerlo operativo.
2. Validar la continuidad de funcionamiento del grupo electrógeno del edificio.
3. Revisar la conectividad / operatividad con el Data Center alternativo en Villa el Salvador en caso requiera entrar en acción.

5) Fallo en el servicio RPVL (Claro)

Acciones si ocurren problemas con el router ubicado en la oficina principal o por problema con la red del proveedor:

- a. Comunicar inmediatamente al proveedor principal del enlace RPVL.
- b. Asegurar que el proveedor alternativo (Americatel) entre en funcionamiento inmediatamente.

En paralelo se deben realizar las siguientes actividades:

1. Realizar seguimiento urgente al proveedor de enlace RPVL para restablecer el servicio.
2. Validar la conectividad / operatividad con el Data Center Alterno en Villa el Salvador en caso requiera entrar en acción.

6) Corte del servicio de Internet (Claro)

Acciones si ocurre una falta de pago del servicio, algún problema con el router ubicado en la oficina principal o algún problema con la red del proveedor:

- a. Comunicar inmediatamente al proveedor principal de Internet.
- b. Asegurar que el proveedor alternativo (Americatel) entre en funcionamiento inmediatamente.

En paralelo se deben realizar las siguientes actividades:

1. Realizar seguimiento urgente al proveedor principal de Internet para restablecer el servicio.
2. Validar la conectividad / operatividad con el Data Center Alterno en Villa el Salvador en caso requiera entrar en acción.
3. Validar la conectividad del enlace brindado por el proveedor alternativo (Americatel).

7) Corte del Sistema SAP

Acciones si ocurre alguna caída por error de programación del mismo sistema SAP o algún problema con el router ubicado en la sede del proveedor que brinda el Hosting y Housing:

- a. Comunicar inmediatamente al proveedor IBM para la revisión del servicio.
- b. Comunicar inmediatamente al proveedor principal de enlace RPVL.
- c. Asegurar que el proveedor alternativo (Americatel) entre en funcionamiento inmediatamente.

En paralelo se deben realizar las siguientes actividades:

1. Realizar seguimiento urgente al proveedor de enlace RPVL para restablecer el servicio.
2. Realizar seguimiento urgente al proveedor IBM para revisar el servicio SAP.
3. Validar que haya conectividad con el sitio de contingencia que brinda el proveedor IBM (pase a su campus San Isidro).
4. Asegurar la conectividad del enlace brindado por el proveedor alternativo (Americatel).

8) Problema de Hardware / Software del sistema de copias de seguridad

Acciones si ocurre una mala realización de la copia de seguridad; problema del servidor a copiar, un mal cálculo de espacio en cinta para el Back-up o por algún problema de cinta malograda:

- a. Validar inmediatamente que la información perdida se encuentre replicada en el Data Center de contingencia (Villa el Salvador) para proceder a recuperarla.
- b. Buscar y restaurar una copia de información (cinta) con más anterioridad que la esperada a la fecha de pérdida.

En paralelo se deben realizar las siguientes actividades:

1. Buscar información perdida en el Data Center alternativo.
2. Solicitar al proveedor custodio las cintas de Back-up para buscar la información más cercana a la fecha de pérdida.
3. Asegurar nuevamente la ejecución de otra copia de seguridad.
4. Validar continuamente las copias de seguridad realizadas mediante pruebas de restauración.

9) Borrado de información en algún servicio utilizado por el usuario final

Acciones si ocurre mal tratamiento de los archivos o por no bloquear las sesiones utilizadas para los diversos servicios por parte de los usuarios:

- a. Validar inmediatamente que la información borrada se encuentre replicada en el Data Center de contingencia (Villa el Salvador) para proceder a recuperarla.
- b. Buscar y restaurar la copia de información más cercana a la fecha de pérdida.

En paralelo se deben realizar las siguientes actividades:

1. Buscar información perdida en el Data Center alternativo.
2. Solicitar al proveedor custodio las cintas de Back-up para buscar información cercana a la fecha de pérdida.

3. Restaurar información a una fecha anterior aceptable.
4. Brindar charlas constantes de concientización a los usuarios para el tratamiento de sus archivos de trabajo.

10) Incidente ocurrido al proveedor custodio en el traslado de copias de seguridad

Acciones en caso se de poca seguridad utilizada para trasladar las copias de la información:

- a. Validar inmediatamente que la información borrada se encuentre replicada en el Data Center de contingencia (Villa el Salvador) para proceder a recuperarla.
- b. Buscar y restaurar una copia de información con más anterioridad que la esperada a la fecha de pérdida.

En paralelo se deben realizar las siguientes actividades:

1. Buscar información perdida en el Data Center alternativo.
2. Solicitar al proveedor custodio las cintas de Back-up anteriores a la fecha de pérdida.
3. Restaurar información a una fecha anterior aceptable.
4. Coordinar penalidad con proveedor custodio por falta grave de pérdida de información.

11) Saturación de procesamiento, memoria y espacio en servidores

Acciones si ocurre una mala configuración de balanceo de carga entre servidores, no hay configuración de alertas en los equipos de monitoreo o por falta de monitoreo por parte del administrador de red:

- a. Validar inmediatamente que la información borrada se encuentre replicada en el Data Center de contingencia (Villa el Salvador) para proceder a recuperarla.
- b. Buscar y restaurar la copia de información más cercana a la fecha de pérdida.

En paralelo se deben realizar las siguientes actividades:

1. Pasar servicios al Data Center alternativo para disminuir la saturación de recursos.
2. Asegurar el monitoreo de recursos por parte del Administrador de Red.

3. Mejorar configuración de alertas para monitorear el uso general de recursos de servidores.
4. Verificar funcionamiento de calidad de servicio (QoS) y ancho de banda (BW) entre Data Centers (principal y alterno).
5. Verificar funcionamiento de servicios de replicación.

12) Problema de réplicas entre servidores de archivos

Acciones si ocurre una mala configuración de las réplicas del servicio DFS:

- a. Solicitar apoyo urgente al proveedor Corporación Sapia para revisar configuración de réplicas.
- b. Buscar y restaurar la copia de información más cercana a la fecha de la última replicación.

En paralelo se deben realizar las siguientes actividades:

1. Revisar funcionamiento del servicio de replicación DFS y Name Space para la distribución de información entre File Servers.
2. Solicitar al proveedor custodio las cintas de Back-up para buscar información cercana a la fecha de última replicación.
3. Documentar tamaños de replicación para llevar un control de información y copias de seguridad.

13) Problema de réplicas del servidor de correo

Acciones si ocurre una mala configuración del servicio DAG para replicación de bases de datos:

- a. Solicitar apoyo urgente al proveedor Corporación Sapia para revisar configuración de réplicas.
- b. Buscar y restaurar la copia de información más cercana a la fecha de la última replicación.

En paralelo se deben realizar las siguientes actividades:

1. Revisar funcionamiento del servicio de replicación DAG de Exchange para la distribución de Bases de Datos de MailBox.
2. Solicitar al proveedor custodio las cintas de Back-up para buscar información cercana a la fecha de última replicación.
3. Documentar tamaños de replicación para llevar un control de información y copias de seguridad.

14) Borrado de archivos importantes de otra área o usuario

Acciones si se presenta un usuario disconforme / molesto / etc.:

- a. Validar inmediatamente que la información borrada se encuentre replicada en el Data Center de contingencia (Villa el Salvador) para proceder a recuperarla.
- b. Buscar y restaurar la copia de información más cercana a la fecha de pérdida.

En paralelo se deben realizar las siguientes actividades:

1. Buscar información perdida en el Data Center alternativo.
2. Solicitar al proveedor custodio las cintas de Back-up para buscar información cercana a la fecha de pérdida.
3. Restaurar información a una fecha anterior aceptable.
4. Revisar continuamente las copias de seguridad realizadas mediante pruebas de restauración.
5. Derivar el caso a Gestión Humana para coordinar sanción.

15) Daño de archivos de algún sistema crítico

Acciones si se presenta un usuario disconforme / molesto / etc.:

- a. Recuperar un servidor físico / virtual necesario para levantar el sistema / aplicación que fue dañada.
- b. Buscar y restaurar la copia de información más cercana a la fecha de pérdida.

En paralelo se deben realizar las siguientes actividades:

1. Implementar un mecanismo de control y monitoreo de acceso / permisos a los archivos del sistema.

16) Ingreso de un atacante a los servicios para borrar y/o robar información de la empresa

Acciones si se presenta un usuario que brinda credenciales de acceso o información confidencial que le sirve al atacante para ingresar a los servicios:

- a. Revisar registros (logs) de accesos para identificar y cerrar puertos y conexiones utilizadas por el atacante.
- b. Cerrar conexiones a los sistemas.
- c. Realizar copias de seguridad de la información y enviarlas urgente al proveedor custodio.

En paralelo se deben realizar las siguientes actividades:

1. Brindar charlas constantes de concientización a los usuarios para poder contrarrestar las técnicas de Ingeniería Social utilizada por los hackers y atacantes.

5.8 Alerta inicial del plan y plantilla de recuperación

En este punto se mostrará de manera general como se desarrollará el procedimiento inicial de alerta y la plantilla para de recuperación del plan de continuidad de servicios críticos de TI.

5.8.1 Diseño de alerta inicial del plan

Todo el personal de la organización que identifique un incidente grave que pueda afectar a los servicios de TI en la empresa, debe comunicarlo inmediatamente a cualquiera de los integrantes del equipo de TI para la continuidad y debe proporcionar el mayor detalle posible con la descripción de los hechos para que se analice y evalúe los escenarios y las acciones que se tomarán.

Además se debe elaborar el documento de declaración del estado de alerta para iniciar el proceso de ejecución del plan de continuidad:

DECLARACIÓN DEL ESTADO DE ALERTA ⁴⁸

Estimado Equipo de TI para la Continuidad:

La suspensión del siguiente servicio crítico y/o servicios críticos de TI: _____, ha superado el tiempo establecido en el umbral de continuidad de dicho(s) servicio(s), el cual fue firmado en el Acuerdo de Nivel de Servicio, por tanto es urgente que se proceda a utilizar el plan de continuidad de servicios críticos de TI para su inmediata restitución.

Saludos cordiales,

Dueño del Servicio

En el caso de que el equipo de TI para la continuidad decidida no activar el plan de continuidad de servicios críticos de TI porque la gravedad del incidente no lo requiere, sí será necesario gestionar de modo urgente el incidente para que no aumente su gravedad y se tenga que aplicar el plan.

5.8.2 Plantilla de recuperación

Después de ejecutado el plan de continuidad de servicios críticos de TI, se debe ejecutar las actividades detalladas en el punto 4.2 ítem c) “Actividades del plan que se deben realizar

⁴⁸ Cfr. Ochoa 2015: 240

después de una interrupción de servicio(s) crítico(s) de TI” para poder documentar los hechos, las acciones tomadas según la estrategia de continuidad elegida de acuerdo a la amenaza.

Se documentará el retorno a la normalidad del servicio crítico de TI conforme a la siguiente plantilla de Ochoa del año 2015:

ACTA DE ENTREGA - RECEPCIÓN DE RETORNO A LA NORMALIDAD DEL SERVICIO CRÍTICO DE TI	
Fecha:	
Lugar:	
Servicio crítico de TI:	
Se suscribe la presente acta entre el responsable de la Gerencia de TI que restableció este Servicio Crítico de TI y el Responsable de dicho servicio consta de las siguientes cláusulas:	
1. OBJETIVO Mantener la continuidad de cada servicio crítico de TI de acuerdo a lo firmado en el Acuerdo de Nivel de Servicio.	
2. ALCANCE Restablecer la continuidad de cada servicio crítico de TI declarado en estado de emergencia, en el menor tiempo posible utilizando el plan de continuidad de dicho servicio.	
3. ESCENARIOS DEL SERVICIO CRÍTICO DE RED	
3.1 Antes de la emergencia	
Emergencia	
Diagnóstico	
3.2 Durante la emergencia	
Detalle de Solución	
3.2 Después de la emergencia	
Normalidad	
4. DERECHOS Y OBLIGACIONES	
4.1 El responsable del servicio verificó que el servicio crítico de TI fue restituido.	
5. FIRMA DE LA ENTREGA - RECEPCIÓN DE RETORNO A LA NORMALIDAD	
5.1 El Responsable de Sistemas y el Responsable del Servicio firman esta Acta en conformidad a las actividades realizadas en la rehabilitación del Servicio y al retorno a la normalidad.	
ENTREGUÉ CONFORME	RECIBÍ CONFORME

Fuente: Plantilla de Ochoa 2015

6 PRUEBAS, RESULTADOS Y VALIDACIÓN

Aquí se mostrarán los resultados de las pruebas del plan de continuidad de TI propuesto en los puntos 4 y 5; de igual forma, se verán los resultados que serán comparados con los indicadores de logro de objetivos que fueron planteados en el punto 2.5 de este proyecto.

6.1 Pruebas del plan de continuidad

La mayoría de las pruebas de continuidad de servicios críticos de TI son de menor escala que una prueba global de continuidad de todas las partes operativas de la empresa. Esto no debe influir para que no se realice una prueba exhaustiva total o parcial ya que el propósito de la prueba de continuidad es determinar hasta qué punto funciona el plan global o qué partes se deben mejorar.

Para la puesta en marcha de la prueba se realizarán las siguientes tareas:

- Verificación de que la información del plan de continuidad es completa y exacta.
- Evaluación del rendimiento del personal involucrado en dicha prueba.
- Evaluación del entrenamiento y percepción por parte de los miembros que no pertenezcan al plan de continuidad.
- Evaluación de la coordinación entre el equipo de contingencia, los proveedores y usuarios de la organización.
- Medición de la habilidad y capacidad del centro de datos alternativo para realizar el proceso de prueba del plan.
- Medición del rendimiento general de las actividades de operaciones y proceso de información relacionados con mantener la capacidad de los servicios críticos de TI para el negocio.

6.1.1 Fases y tipos de pruebas

Primero se realizará una **prueba** que es la acción real de probar el plan de contingencia. Se probará la alta disponibilidad, llamadas telefónicas, proceso de datos, órdenes de transporte y movimiento de personal y proveedores. Los evaluadores realizarán un examen del personal

involucrado mientras realizan las tareas designadas. Esta es la prueba que indica el nivel de preparación de la organización para responder a la emergencia.

Luego se realizará una **posprueba** que consiste en la limpieza de las actividades realizada en la fase de prueba. Esta posprueba comprende actividades como devolver todos los recursos a su lugar correcto, volver a establecer conexiones y retorno del personal, así como evaluar formalmente el plan e implementar las mejoras indicadas.

Asimismo, según las buenas prácticas se pueden realizar los siguientes tipos de pruebas:

- a. Prueba sobre papel o de escritorio: Consiste en un recorrido del plan sobre papel, haciendo participar a los principales involucrados en la ejecución del plan, quienes razonan lo que podría suceder en el caso de una determinada paralización de servicio.
- b. Prueba de nivel de preparación: Es una versión restringida de la prueba completa. Esta prueba se hace periódicamente sobre diferentes aspectos o partes del plan, y puede ser una forma eficiente de obtener gradualmente evidencia sobre cuán bueno es el plan. También sirve para proveer un medio para mejorar el plan gradualmente.
- c. Prueba operativa completa: La organización debe haber probado bien el plan sobre papel y a nivel de preparación antes de poner en marcha esta última prueba. Esto se realiza con el fin de probar cómo se respondería ante una paralización o desastre. En esta prueba se simula el desastre como si éste efectivamente hubiere ocurrido.

En el caso de este proyecto se realizará la simulación de paralización y pruebas iniciales de cada una ellas para luego generar informes y poder comparar los resultados con los objetivos específicos.

6.1.2 Plan de pruebas

Para este proyecto, se ha definido el siguiente plan de pruebas:

6.1.2.1 ¿Qué se probará?

Con el plan de pruebas, se probará y validará que los tres servicios críticos de TI de la organización puedan continuar operando y sean recuperados en los tiempos propuestos y

tolerables por la organización; además que dichos tiempos sean menores a los que se tenían considerados antes.

1. **En los servidores de archivos:** se probará que se tenga continuidad del servicio con el correcto funcionamiento del rol DFS y NameSpace de Microsoft, para que en caso se presente alguna caída de los servidores de archivos en la oficina principal, puedan entrar en funcionamiento los servidores replicados en el Centro de Datos alterno.
2. **En el sistema SAP:** se probará que la continuidad propuesta por el proveedor IBM funcione correctamente, además de que se cumplan los tiempos acordados de continuidad y recuperación del servicio.
3. **En el correo electrónico:** se probará que se mantenga la continuidad del servicio con el correcto funcionamiento del rol DAG de Microsoft, para que en caso se dé una caída del servidor principal de correo, pueda entrar en funcionamiento el servidor replicado en el Centro de Datos alterno.
4. **El nivel de conocimiento de los usuarios de la organización:** se probará cómo actuarían los usuarios de la organización en caso se presente una paralización general de los servicios que ellos utilizan. Por ejemplo, cómo continuarían sus operaciones en caso de no tener correo electrónico.
5. **El nivel de conocimiento del equipo de TI:** se probará que el equipo de TI tenga el conocimiento de qué procedimientos y actividades seguir para poder recuperar y luego restaurar los servicios críticos de TI; se validará que estas pruebas sean realizadas en los tiempos tolerables por la organización.

6.1.2.2 Escenarios de pruebas

Tendremos los siguientes escenarios de pruebas:

1. **Para los servidores de archivos:** se lleva a cabo una prueba coordinada desconectando las carpetas de red “Mis documentos” de varios usuarios de la organización. En este escenario tenemos al servidor OPFS07 que se encuentra en la Oficina Principal (Data Center Principal en Miraflores) y también tenemos al servidor UDEFS07 que se encuentra alojado en el Almacén Central (Data Center Alterno en Villa el Salvador).
2. **Para el sistema SAP:** se hace una prueba coordinada con el proveedor IBM para que se realice un corte de servicio de sus servidores en su Data Center principal (La Molina)

y que entre en operación sus servidores en su Data Center alternativo (San Isidro). Se validará que las Bases de Datos estén replicadas correctamente y que el sistema funcione de manera estable.

3. **Para el correo electrónico:** se lleva a cabo una prueba coordinada junto con el apoyo del proveedor Corporación Sapia para realizar un corte de servicio que simule un caída del servidor de correo electrónico principal (OPEXMBX02) y para que entre en funcionamiento el servidor secundario (OPECMBX03) que está en Villa el Salvador con las bases de datos replicadas. El servicio debe continuar de modo transparente para los usuarios.
4. **Para ver el nivel de conocimiento de los usuarios de la organización:** se lleva a cabo una prueba con las consultas adecuadas que muestran un escenario de caída de servicios y ver cómo actuarían los usuarios para poder continuar sus procesos de trabajo sin tener sus servicios críticos.
5. **Para ver el nivel de conocimiento del equipo de TI:** se realiza una prueba con las preguntas y consultas adecuadas sobre qué pasos y actividades seguiría un personal responsable de un servicio crítico para poder recuperar y restaurar el servicio.

6.1.2.3 Modalidad o tipo de prueba

Recordemos que en el punto 6.2 Fases y Tipos de Pruebas, definimos tres tipos de pruebas para el plan de continuidad de servicios de TI. Todas estas pruebas que se llevarán a cabo se darán principalmente en la modalidad Prueba de Nivel de Preparación y en Prueba sobre Papel o de Escritorio. En parte también, se hará la Prueba Operativa Completa ya que es necesario tener ambas pruebas anteriores completas.

Para nuestro caso, son suficientes las dos primeras pruebas para obtener indicadores de estado del plan y de mejora. A continuación se detalla el tipo de prueba en cada servicio.

1. **Para los servidores de archivos:** se hará una prueba de nivel de preparación y prueba operativa completa.
2. **Para el sistema SAP:** se realizará una prueba de nivel de preparación y prueba operativa completa.
3. **Para el correo electrónico:** se llevará a cabo una prueba de nivel de preparación y prueba operativa completa.

4. **Para ver el nivel de conocimiento de los usuarios de la organización:** se hará una prueba de escritorio.
5. **Para ver el nivel de conocimiento del equipo de TI:** se llevará a cabo una prueba de escritorio.

6.1.2.4 Fechas de las pruebas

En diferentes fechas del año 2017, el equipo de TI ha realizado simulaciones de corte de cada servicio crítico con evidencias para poner en prueba el plan de continuidad.

1. **Para los servidores de archivos:** 20 de Enero de 2017 con 03 horas de ventana.
En la mañana a partir de las 09:00 a.m. y antes de las 12:00 p.m.
2. **Para el sistema SAP:** 23 y 24 de Febrero de 2017 con 08 horas de ventana.
En la noche del día 23/02 a partir de las 10:00 p.m. y en la madrugada del día 24/02.
3. **Para el correo electrónico:** 14 de Junio de 2017 con 07 horas de ventana.
En la madrugada a partir y parte de las 12:00 a.m. y a primeras horas de la mañana.
4. **Para ver el nivel de conocimiento de los usuarios de la organización:** 27 y 28 de Junio de 2017. En la mañana y en la tarde de ambos días para distribuir por áreas.
5. **Para ver el nivel de conocimiento del equipo de TI:** 30 de Junio 2017 y 01 de Julio de 2017. En la mañana y en la tarde de ambos días ya que el equipo de TI no tiene un tiempo determinado para completar su prueba.

6.1.2.5 Personal responsable en las pruebas

- **El equipo de TI:** Tendrán básicamente dos tareas; en primer lugar evaluar a los usuarios de la organización para que en base a los resultados, se les capacite, oriente o indique cómo actuar ante una paralización. En segundo lugar, tener el conocimiento de qué procesos seguir para ejecutar el plan de continuidad tanto en las pruebas como en un escenario real; es decir, desde tener la documentación lista, coordinar con los proveedores, habilitar servidores de contingencia, validar servicios recuperados, y por último documentar la paralización que ocurrió para que sirva como experiencia en el futuro.

6.1.3 Ejecución de pruebas

6.1.3.1 Para los servidores de archivos

Aquí nos enfocaremos en la carpeta “Mis documentos” del usuario whuaman que se encuentra alojada en el servidor OPFS07 habilitado con el servicio DFS y NameSpace de Microsoft para brindar alta disponibilidad de los servidores de archivos.

Al realizar dicha prueba, veremos en la siguiente imagen enviada por correo electrónico por el mismo usuario, como se desconecta su carpeta “Mis documentos” del servidor principal (OPFS07) y luego en pocos minutos, entra en funcionamiento la carpeta replicada en el servidor que está en Villa el Salvador (UDEFS07).

Nota: El corte es realizado el día 20 de enero de 2017 minutos antes de las 09:35 a.m. Aproximadamente a las 09:30 a.m.

Evidencia de correo electrónico enviado por el usuario WHuaman

De: Wilfredo Huamán Velásquez

Enviado el: miércoles, 20 de enero de 2017 09:35 a.m.

Para: Reich Sánchez Torres; Consultor 11 - TI

CC: Renzo Correa Salazar

Asunto: Mis documentos

Figura 7. Evidencia de sincronización de file server en sitio alterno

Fuente: JJC Contratistas Generales S.A.

Atentamente.

WILFREDO J. HUAMÁN VELÁSQUEZ
Analista de Proyectos
JJC Contratistas Generales S.A.
Av. Alfredo Benavides 768
Lima 18 – Perú
T. +614-1300 Ext. 1212
RPC. +999.029.884

Luego el usuario continua trabajando así durante unos minutos (con menor rendimiento, pero sí logra trabajar). Unos diez minutos después en el área de TI se reactiva el servidor OPFS07

de la Oficina Principal (con rendimiento normal) como vemos en otro correo enviado por el usuario.

Evidencia de correo electrónico enviado por el usuario WHuaman

De: Wilfredo Huamán Velásquez

Enviado el: miércoles, 20 de enero de 2017 09:45 a.m.

Para: Reich Sánchez Torres; Consultor 11 - TI

CC: Renzo Correa Salazar

Asunto: RE: Mis documentos

Reinicié y ya apareció así:

Figura 8. Evidencia de sincronización de file server en sitio principal

Fuente: JJC Contratistas Generales S.A.

Por último, el administrador de red RSanchez pide la confirmación del rendimiento del servidor cuando se retorna el servicio desde la Oficina Principal:

Evidencia de correo electrónico enviado por el Administrador de Red RSanchez

De: Reich Sánchez Torres

Enviado el: miércoles, 20 de enero de 2017 09:54 a.m.

Para: Wilfredo Huamán Velásquez; Consultor 11 - TI

CC: Renzo Correa Salazar; Alexander Carlos Blanco Panduro; Consultor 11 - TI

Asunto: RE: Mis documentos

Wili ahora está más rápido?

Enviado desde mi Samsung Mobile de Claro

Evidencia de respuesta de correo electrónico del usuario WHuaman

De: Wilfredo Huamán Velásquez

Enviado el: miércoles, 20 de enero de 2017 09:58 a.m.

Para: Reich Sánchez Torres; Consultor 11 - TI

CC: Renzo Correa Salazar; Alexander Carlos Blanco Panduro; Consultor 11 - TI

Asunto: RE: Mis documentos

Reich:

Sí está más rápido.

WHV

El proceso de la prueba en general toma un promedio de una hora, pero cada cambio de servidores ubicados en diferentes Centros de Datos toma como máximo 20 minutos.

6.1.3.2 Para el sistema SAP

En el caso del sistema SAP, se realiza una prueba de corte programada con el proveedor IBM para que entre en funcionamiento la alta disponibilidad del sistema SAP.

Figura 9. Evidencia de correo electrónico enviado por la Mesa de Ayuda de JJC para avisar a los usuarios el corte del sistema SAP. En interno se hará la prueba de continuidad

Fuente: JJC Contratas Generales S.A.

Junto con IBM se realiza la prueba coordinada y en la siguiente gráfica podemos ver cómo continúan las operaciones estables poco más de las 06:00 a.m. Luego a las 08:00 a.m. aumenta el uso del sistema SAP cuando los usuarios comienzan a trabajar normalmente.

Figura 10. Gráfica de monitoreo Cacti para ver la conexión a SAP en servidores alternos de IBM

Fuente: JJC Contratistas Generales S.A.

La prueba en general tiene una ventana máxima de 8 horas máximo (como se indica en el correo enviado por Mesa de Ayuda) para que entren en funcionamiento los servidores alternos de IBM, pero el proceso en sí toma una hora como máximo.

6.1.3.3 Para el correo electrónico

En el caso del correo electrónico, se realiza una prueba de corte programada con el proveedor Corporación Sapia para asegurar el servicio DAG de Microsoft para brindar alta disponibilidad entre las bases de datos del Servidor Exchange.

Evidencia de correo electrónico enviado por el especialista JRecuay de Corporación Sapia

De: José Recuay Yanayaco [<mailto:jrecuay@cosapidata.com.pe>]

Enviado el: martes, 14 de junio de 2017 01:17 a.m.

Para: Reich Sánchez Torres <rsanchez@jjc.com.pe>; Alexander Carlos Blanco Panduro <ablanco@jjc.com.pe>

CC: Sandro Mina Valdivia <smina@cosapidata.com.pe>; Alexia Fuller Marquez <afuller@cosapidata.com.pe>; Renzo Correa Salazar <rcorrea@jjc.com.pe>; Sergio Geldres Reategui <sgeldres@cosapidata.com.pe>; Giovanni Angeles Segama <gangeles@cosapidata.com.pe>; Carlos Urquizo Urquizo <curquizo@cosapidata.com.pe>; José Navarro Rojas <jnavarro@cosapidata.com.pe>

Asunto: RE: Inicio de Actividades - Actualización de Servidores

Estimado Alex:

Por favor, apoyarme confirmándome si se completaron las réplicas de las BDs hacia la sede secundaria (DSG).

A la espera de sus comentarios

Saludos Cordiales

Atte.,

José Luis Recuay Yanayaco

UN Soluciones Microsoft

F (511) 215 4540

C (51) 999 913 756

Av. Coronel Andrés Reyes 420
piso 10.

San Isidro

<http://www.cosapidata.com.pe>

Evidencia de respuesta del correo electrónico enviado por el Administrador de Red ABlanco

De: Alexander Carlos Blanco Panduro

Enviado el: martes, 14 de junio de 2017 08:59 a.m.

Para: José Recuay Yanayaco; Reich Sánchez Torres

CC: Sandro Mina Valdivia; Alexia Fuller Marquez; Renzo Correa Salazar; Sergio Geldres Reategui; Giovanni Angeles Segama; Carlos Urquizo Urquizo; José Navarro Rojas

Asunto: RE: Inicio de Actividades - Actualización de Servidores

Hola José,

Confirmado, ya completó las réplicas de las bases de datos (ver imagen).

PS C:\>Get-MailboxDatabaseCopyStatus -Server OPECMEX03 | FT

Name	Status	CopyQueue Length	ReplayQueue Length	ContentIndex State
ingenieria02\OPECMEX03	Healthy	0	0	Healthy
Comercia102\OPECMEX03	Healthy	0	0	Healthy
SERVICIOS\OPECMEX03	Healthy	0	1	Healthy
Gerencia01\OPECMEX03	Healthy	0	0	Healthy
GERENCIA01P001\OPECMEX03	Healthy	0	0	Healthy
GERENCIA01P01\OPECMEX03	Healthy	0	0	Healthy
CONSORCIO2\OPECMEX03	Healthy	0	1	Healthy
EDIFICACIONES\OPECMEX03	Healthy	0	0	Healthy
GERENCIA001\OPECMEX03	Healthy	0	0	Healthy
GERENCIA01P02\OPECMEX03	Healthy	0	0	Healthy
SERVICIOS02\OPECMEX03	Healthy	0	0	Healthy
GERENCIA01P04\OPECMEX03	Healthy	0	0	Healthy
GERENCIA01P05\OPECMEX03	Healthy	0	0	Healthy
DP03\OPECMEX03	Healthy	0	1	Healthy
DBRAS02\OPECMEX03	Healthy	0	0	Healthy
DBRAS03\OPECMEX03	Healthy	0	0	Healthy
DP01\OPECMEX03	Healthy	0	0	Healthy
DBRAS04\OPECMEX03	Healthy	0	0	Healthy
LICSO1\OPECMEX03	Healthy	0	0	Healthy
DBRAS06\OPECMEX03	Healthy	0	0	Healthy
GERENCIA01P03\OPECMEX03	Healthy	0	0	Healthy
DP02\OPECMEX03	Healthy	0	0	Healthy
DBRAS08\OPECMEX03	Healthy	0	0	Healthy
Cesados\OPECMEX01	FailedAndSus...	464222	0	Failed
IME1\OPECMEX03	Healthy	0	0	Healthy
MUELLE1\OPECMEX03	Healthy	0	0	Healthy
DBRAS04\OPECMEX03	Healthy	0	0	Healthy
DBRAS05\OPECMEX03	Healthy	0	0	Healthy
DBRAS07\OPECMEX03	Healthy	0	0	Healthy
DP04\OPECMEX03	Healthy	0	0	Healthy
DP05\OPECMEX03	Healthy	0	0	Healthy
DP06\OPECMEX03	Healthy	0	0	Healthy
RECURSOS1\OPECMEX03	Healthy	0	0	Healthy
IDE\OPECMEX03	Healthy	0	0	Healthy
CONSORCIO1\OPECMEX03	Healthy	0	1	Healthy
GERENCIA0BRAS\OPECMEX03	Healthy	0	0	Healthy
AGROPECUARIAS\OPECMEX03	Healthy	0	0	Healthy
SERVICIOS01\OPECMEX03	Healthy	0	0	Healthy
DBRAS_LIMBOM\OPECMEX03	Healthy	0	0	Healthy
Mat\OPECMEX03	Mounted	0	0	Healthy
OFICINA\OPECMEX03	Healthy	0	0	Healthy
OFICINAPRINCIPAL01\OPECMEX03	Healthy	0	0	Healthy
CONSORCIO3\OPECMEX03	Healthy	0	0	Healthy
Cesados1\OPECMEX03	Healthy	0	0	Healthy
ingenieria03\OPECMEX03	Healthy	0	1	Healthy
ingenieria04\OPECMEX03	Healthy	0	0	Healthy
IME2\OPECMEX03	Healthy	0	0	Healthy
Cesados Sin Contenido\OPECMEX03	Healthy	0	0	Healthy
OFICINAPRINCIPAL02\OPECMEX03	Healthy	0	0	Healthy
OFICINAPRINCIPAL03\OPECMEX03	Healthy	0	0	Healthy
OFICINAPRINCIPAL04\OPECMEX03	Healthy	0	0	Healthy
Comercia103\OPECMEX03	Healthy	0	0	Healthy

Figura 11. Evidencia de replicación de las bases de datos de correo electrónico al sitio alterno

Fuente: JJC Contratistas Generales S.A.

Gracias,

Alex Blanco
Tecnologías de la Información
JJC Contratasistas Generales S.A.
Av. Alfredo Benavides 768
T. +614 1300 Ext. 1445
C. + 989591991

Figura 12. Gráfica de monitoreo Cacti para ver la réplica de las bases de datos de correo electrónico en los servidores alternos que están en Villa el Salvador

Fuente: JJC Contratasistas Generales S.A.

El proceso de la prueba en general toma un promedio de 7 horas, pero cada cambio de servidores ubicados en diferentes Centros de Datos toma como máximo 2 horas.

Además el equipo de TI debe asegurar que se tengan preparadas las copias de seguridad de cada servidor debidamente documentadas y con las pruebas de restauración hechas en determinados periodos.

A continuación mostraremos evidencias de una prueba de restauración semestral y de la documentación de Back-ups mensuales (completos) y diarios (incrementales):

DOCUMENTACIÓN DE RESTAURACIÓN DE INFORMACIÓN	
PROCESO DE RESTAURACIÓN:	
Usuario(s): Carlos Torres – Gestor de Soluciones TI Henry Falcon – Practicante Preprofesional TI Carlos Quispe – Consultor de Transligna Soluciones Integrales Reich Sánchez Torres – Administrador de Red	Área / Empresa: TI / JJC
Motivo de restauración: Prueba de restauración semestral de la Base de Datos OnBase Lab que está dentro del motor de base de datos SQL Server en producción OPSQLR201. (Mes de Junio 2017).	Fecha de solicitud: 15 / 06 / 2017
	Fecha de restauración: 15 / 06 / 2017
Ubicación / ruta de los archivos: <i>(Indicado por el usuario)</i> Servidor de SQL de Aplicaciones (OPSQLR201)	
Nombres de carpetas y/o archivos: <i>(Indicado por el usuario)</i> Se restaurará toda la información de la Base de Datos OnBase Lab que está dentro del motor de base de datos SQL Server en producción OPSQLR201 (Backup_Full mes de Junio 2017).	
Fecha y Hora: <i>(Detallar en caso sea una restauración de información borrada)</i> Para acercar a un escenario real, se eliminó la BD original (OnBaseLab) y se procedió a restaurar la BD desde la cinta de backup	
Ubicación de los archivos y carpetas restaurados: Motor de base de datos de SQL Server – Instancia: OPSQLR201\opsqsp2010\OnBaseLab	
Tamaño total de información restaurada: 127 GB	
CONFORMIDAD:	
Observación: Firma del Gerente / Jefe / Solicitante / Involucrados Firma del Operador de Backup REICH SÁNCHEZ TORRES	

Figura 13. Evidencia de prueba de restauración semestral de Back-up de Bases de Datos SQL en el mes de Junio del año 2017

Fuente: JJC Contratistas Generales S.A.

Figura 14. Gráfica de documentación de estado de Back-ups mensuales (completos) por cada servidor en el año 2017

Fuente: JJC Contratistas Generales S.A.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI		
	CINTAS:	TAMAROS 1 DÍAS (GB)																																		
Slot Robot	SERVIDORES	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	TOTAL X SERVIDOR	OBSERVACIONES		
8	EXCHANGE-DAG	29.40	17.10	20.10	14.60	48.90	61.10	60.80	54.80	52.90	25.60	26.10	60.80	153.00	147.00	53.90	16.90	36.10	51.50	0.00	57.40	62.60	63.20	61.50	29.40	16.40	57.00	58.50	62.10	29.30	59.70	29.30	1537.00	OK		
11.1	OPAP1	2.83	0.36	0.62	0.92	5.00	4.59	7.72	7.38	6.77	4.21	0.70	9.43	6.86	6.62	7.51	6.92	1.03	6.16	0.94	6.19	5.74	5.40	6.17	2.68	1.61	6.43	6.09	2.21	5.89	5.70	0.63	142.32	OK		
11.2	MDB2Legacy														30.20																		151.20	Revisar		
21.1	OPFS01_Ingenieria	0.01	0.00	0.00	0.01	0.18	1.97	0.40	71.40	0.10	0.00	0.00	12.70	0.09	0.07	0.62	0.47	0.00	0.00	0.00	0.98	0.00	1.56	8.37	0.07	0.00	0.71	0.00	0.05	11.90	1.67	0.00	113.33	OK		
13.1	OPFS01_Urvariar (A-T) + Urvariar18	0.23	0.00	0.00	0.00	1.19	0.92	1.90	2.18	0.39	0.01	0.01	0.80	0.84	2.98	0.60	0.91	0.00	0.00	1.70	0.27	0.86	0.33	0.72	0.00	0.00	3.11	2.24	0.21	9.19	0.71	0.03	32.34	OK		
14.1	OPFS01_Urvariar (U-Z) + E/Uroz-G	3.01	0.00	1.92	0.98	1.59	3.52	17.50	3.55	2.09	0.24	0.00	3.80	6.33	2.22	1.91	1.90	0.00	0.00	5.32	0.10	3.83	2.68	3.17	1.38	0.00	2.15	2.85	1.58	1.88	1.78	0.00	77.28	OK		
12	OPFS01_Departamentar	0.02	0.00	0.00	0.00	0.28	3.16	9.86	1.95	6.58	0.00	0.00	7.54	1.00	0.55	1.83	0.66	0.00	0.00	389.00	0.91	102.00	0.18	0.51	0.01	0.00	1.76	0.00	0.06	0.27	1.26	0.00	529.39	OK		
9.1	OPFS02_D	17.60	0.00	0.00	0.00	17.70	2.74	17.30	17.80	17.70	17.60	0.00	17.70	0.01	17.70	18.10	17.70	0.00	17.60	17.70	17.70	17.70	17.70	17.70	0.00	0.00	17.90	0.00	17.70	17.80	17.90	0.00	357.55	OK		
9.2	OPFS02_E	0.03	0.00	0.00	0.00	1.91	0.04	26.60	0.91	10.80	0.00	0.00	9.95	6.15	0.57	0.03	0.45	0.00	0.00	0.64	10.90	8.36	8.29	2.85	0.00	0.00	8.12	0.00	12.20	17.60	19.70	0.00	146.10	OK		
19.3	OPFS02_G	0.05	0.00	0.00	0.00	0.10	0.46	0.09	9.64	0.09	0.00	0.00	0.01	6.37	0.01	0.06	0.13	0.00	0.00	0.13	0.33	16.30	0.07	0.29	0.00	0.00	3.37	0.00	0.43	0.17	0.19	0.00	38.29	OK		
10	OPFS03_E	0.00	0.00	0.00	0.00	0.15	33.80	0.32	0.36	1.32	0.00	0.00	0.21	1.98	0.68	1.20	1.05	0.00	2.07	0.00	0.45	6.92	0.18	0.74	0.00	0.00	2.23	0.00	0.03	12.70	8.59	0.00	74.98	OK		
19.4	OPFS03_F-E																																0.00	OK		
19.1	OPFS04	0.02	0.00	0.00	0.00	0.19	1.85	0.32	6.95	2.43	0.00	0.00	0.21	1.10	1.01	0.06	0.26	0.00	0.00	0.00	2.79	0.11	0.48	0.13	0.00	0.00	0.05	0.00	0.12	3.09	0.09	0.00	21.26	OK		
19.5	OPFS05																																0.00	OK		
13.2	OPFS06																																0.00	OK		
14.3	OPFS07																																0.00	OK		
22.1	OPFS08																																0.00	OK		
15.3	UDEFS01	0.00	0.75	0.00	0.99	0.78	1.14	0.24	0.15	0.27	0.00	0.30	1.00	1.12	1.19	1.74	0.78	0.00	1.26	1.28	1.35	1.44	1.49	0.75	0.00	1.62	1.62	1.71	1.79	1.11	0.76	0.00	26.62	OK		
19.2	UDEFS02	0.09	0.00	0.06	0.00	0.05	0.11	0.04	0.01	0.05	0.27	0.00	0.06	0.08	0.20	0.04	0.24	0.00	0.00	1.66	0.00	0.54	0.16	0.10	0.11	0.00	0.48	142.00	0.42	0.40	0.11	0.09	147.37	OK		
14.2	OPDFS01_D	0.00	0.00	0.00	0.00	0.12	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	4.50	0.27	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	11.78	OK		
15.4	OPDFS01_F	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	OK		
15.5	OPDFS01_G																																0.00	OK		
15.2	OPDC01		10.90			10.90			10.90				16.90			16.90				10.90				16.90				16.90				11.00	122.20	Revisar		
16.4	OPDC02	0.59	0.83	0.59	0.74	0.76	0.95	0.73	0.75	0.90	0.70	1.16	0.78	0.93	0.85	0.72	0.74	0.00	0.95	0.81	0.96	0.73	1.02	0.67	0.66	0.71	0.73	1.10	0.68	0.72	0.68	0.62	23.76	OK		
16.2	OPINTRANET	0.54	0.48	0.46	0.44	0.50	0.46	0.48	0.48	0.50	0.49	0.45	0.43	50.00	1.36	0.96	0.93	0.00	0.00	0.00	0.46	0.89	0.89	0.94	0.95	0.88	0.91	0.92	0.91	0.91	0.96	0.92	69.48	OK		
16.5	OPISCO	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.05	0.02	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	OK		
16.1	OPSP01	24.40						24.40								24.40							24.50							24.60			122.30	Revisar		
21.3	OPFS09																																0.00	Revisar		
16.3	OPCOMHIST																																0.00	Revisar		
17	OPSOLR201				827.00														827.00														1710.00	Revisar		
18.1	ORACLE											550.00															416.00						966.00	Revisar		
18.2	ONBASE		256.00			256.00				256.00			256.00			256.00			256.00					256.00			256.00				256.00		2304.00	Revisar		
18.3	S10 JJC																																152.60	Revisar		
18.4	S10 JJC-SC						73.50															73.50											147.00	Revisar		
18.5	OPMAR01								0.87															0.88									1.75	Revisar		
15.1	OPBACKUP01															105.00																	105.00	Revisar		
21.2	OPINGHIST																																0.00	Revisar		
22.2	OPSAFEPSBACKUP																																0.00	Revisar		
	TOTAL X DIA X CINTA (GB)	79.81	286.42	23.75	901.69	335.39	201.20	144.79	203.58	369.79	49.12	578.71	401.42	328.85	213.21	225.17	323.35	54.83	888.94	675.13	189.71	228.29	129.01	377.50	35.26	437.22	342.56	308.81	222.50	137.53	375.81	42.60				
	INCORRECTO - FALLO																																			
	COMPLETO CON ERROR																																			
	CANCELADO																																			
	OMITIDO																																			

Figura 15. Cuadro de documentación de estado de Back-ups diarios (incrementales) en un mes del año 2017

Fuente: JJC Contratistas Generales S.A.

Todo el equipo de TI es responsable del plan de continuidad de servicios de TI. Son los que han realizado las pruebas y las documentaciones antes mencionadas. Además serán los que revisarán que los usuarios sepan cómo deberían actuar en caso de la paralización de servicios a través de la prueba de escritorio. El equipo de TI también realizará la prueba general del plan de continuidad.

Tabla 22

Equipo de TI que validará las pruebas de escritorio

Nro	USUARIO	EMPRESA	ÁREA	CARGO	PRUEBA Y VALIDACIÓN DE SERVICIO
202	Alexander Carlos Blanco Panduro	JJC CONTRATISTAS GENERALES S.A.	TECNOLOGIA DE LA INFORMACION	ADMINISTRADOR DE REDES Y COMUNIC. I	Sistema SAP / Correo electrónico / File Server y demás servicios
204	Ángela María Carrasco Burneo	JJC CONTRATISTAS GENERALES S.A.	TECNOLOGIA DE LA INFORMACION	GERENTE TECNOLOGIAS DE INFORMACION	Sistema SAP / Correo electrónico / File Server y demás servicios
209	Elvis Porras Poma	JJC CONTRATISTAS GENERALES S.A.	TECNOLOGIA DE LA INFORMACION	JEFE DE SOPORTE TECNOLÓGICO	Sistema SAP / Correo electrónico / File Server y demás servicios
210	Fernando Boza Gonzalez	JJC CONTRATISTAS GENERALES S.A.	TECNOLOGIA DE LA INFORMACION	JEFE SENIOR DE SERVICIOS TECNOLÓGICOS	Sistema SAP / Correo electrónico / File Server y demás servicios
211	Geo Baccarani Rosas	JJC CONTRATISTAS GENERALES S.A.	TECNOLOGIA DE LA INFORMACION	JEFE DE SISTEMAS	Sistema SAP / Correo electrónico / File Server y demás servicios
221	Reich Sánchez Torres	JJC CONTRATISTAS GENERALES S.A.	TECNOLOGIA DE LA INFORMACION	ADMINISTRADOR DE REDES Y COMUNIC. II	Sistema SAP / Correo electrónico / File Server y demás servicios
222	Renzo Giancarlo Correa Salazar	JJC CONTRATISTAS GENERALES S.A.	TECNOLOGIA DE LA INFORMACION	ADMINISTRADOR DE REDES Y COMUNIC. I	Sistema SAP / Correo electrónico / File Server y demás servicios

Fuente: Elaboración propia con información de JJC Contratistas Generales

6.1.3.4 Pruebas de escritorio

Para poder realizar la prueba de escritorio, se han elaborado dos plantillas para poder conocer cómo actuarían los usuarios de la organización y que cómo lo haría el equipo de TI.

Ejemplo de prueba de escritorio para los usuarios de JJC Contratistas Generales

Estimado Usuario:

Por favor responda las siguientes preguntas:

En el caso de que exista una paralización de los servicios de TI que usted utiliza, por ejemplo si el sistema SAP no funciona, ¿cuál sería el proceso que Usted realizaría para continuar con sus labores?

1.- ¿Cómo continuar mi trabajo si no tengo el servidor donde guardo mis archivos?

2.- ¿Cómo continuar mi trabajo si no tengo el sistema SAP?

3.- ¿Cómo continuar mi trabajo si no tengo correo electrónico?

Fuente: Elaboración propia

Ejemplo de prueba de escritorio para el equipo de TI de JJC Contratistas Generales

Estimado Personal del Equipo de TI:

Si se produce una paralización repentina de algún servicio de TI que Usted es responsable, supervisa y monitorea, mencione y ordene las acciones y pasos que debería seguir para ejecutar el plan de continuidad de servicios críticos de TI.

1.- Para los Servidores de Archivos:

2.- Para el Sistema SAP:

3.- Para el Correo Electrónico:

Fuente: Elaboración propia

Para la prueba de escritorio a realizar a los usuarios de la organización, se ha seleccionado entre dos a tres trabajadores clave de cada área para poder saber cuáles serían las acciones que tomarían en determinados servicios, los avisos que deberían realizar o los procesos que deberían hacer en caso se paralicen los servicios de TI que ellos utilizan.

Tabla 23

Usuarios seleccionados para las pruebas de escritorio

Nro.	USUARIO	EMPRESA	ÁREA	CARGO	PRUEBA DE SERVICIO
1	Adrián Scarafia	JJC CONTRATISTAS GENERALES S.A.	ADMINISTRACION	GERENTE CENTRAL ADM. Y FINANZAS	Correo electrónico
3	Yasmin Ojeda Flores	JJC CONTRATISTAS GENERALES S.A.	ADMINISTRACION	JEFE DE ADMINISTRACION	Correo electrónico / File Server
10	Manuel Chamochumbi Livelli	JJC CONTRATISTAS GENERALES S.A.	ADMINISTRACION DE CONSORCIOS	CONTADOR DE CONSORCIO II	Sistema SAP / Correo electrónico / File Server
11	María Esther Palomino de la Cruz	JJC CONTRATISTAS GENERALES S.A.	ADMINISTRACION DE CONSORCIOS	CONTADOR DE CONSORCIO II	Sistema SAP / Correo electrónico / File Server
19	Elena Alarcón Ledesma	JJC CONTRATISTAS GENERALES S.A.	ARCHIVO	JEFE DE DOCUMENTACIÓN Y ARCHIVO	File Server
23	Manuel Alejandro Tueros Jurado	JJC CONTRATISTAS GENERALES S.A.	ARCHIVO	ASISTENTE DE ARCHIVO	File Server
25	Ricardo Cochachi Taipe	JJC CONTRATISTAS GENERALES S.A.	AUDITORIA INTERNA	AUDITOR INTERNO II	Correo electrónico / File Server
33	Isabel Armas Durand	JJC CONTRATISTAS GENERALES S.A.	COMERCIAL	ANALISTA COMERCIAL I	Correo electrónico / File Server
35	Néstor Martínez Levano	JJC CONTRATISTAS GENERALES S.A.	COMERCIAL	GERENTE COMERCIAL	Correo electrónico / File Server
39	David Gamarra Alarco	JJC CONTRATISTAS GENERALES S.A.	COMUNICACIONES	ASISTENTE DE COMUNICACIONES I	File Server
40	Elizabeth Uribe Arroyo	JJC CONTRATISTAS GENERALES S.A.	COMUNICACIONES	JEFE DE COMUNICACION E IMAGEN CORPORATIVA	Correo electrónico / File Server
49	José Eduardo Chávez Campos	JJC CONTRATISTAS GENERALES S.A.	CONTABILIDAD	JEFE SENIOR DE CONTABILIDAD	Sistema SAP / Correo electrónico / File Server
52	Luis Laya Cavero	JJC CONTRATISTAS GENERALES S.A.	CONTABILIDAD	JEFE DE CONTROL PATRIMONIAL	Sistema SAP / File Server
55	Pierre Acuña Dávila	JJC CONTRATISTAS GENERALES S.A.	CONTABILIDAD	ASISTENTE CONTABLE II	Sistema SAP / File Server
60	David Michelón	JJC CONTRATISTAS GENERALES S.A.	CSSM	COORDINADOR DE GESTION INTEGRADA II	Correo electrónico / File Server
63	Enrique Hugo Quispe Huamán	JJC CONTRATISTAS GENERALES S.A.	CSSM	JEFE MEDICO OCUPACIONAL	File Server
65	María Del Pilar Gutiérrez	JJC CONTRATISTAS GENERALES S.A.	CSSM	JEFE DE SISTEMA INTEGRADO DE CSSM	Correo electrónico / File Server
69	Antonio Túpac Yupanqui Sarapura	JJC CONTRATISTAS GENERALES S.A.	FINANZAS	JEFE DE TESORERÍA	Sistema SAP / Correo electrónico / File Server
70	Edward Román Gutiérrez	JJC CONTRATISTAS GENERALES S.A.	FINANZAS	ASISTENTE ADMINISTRATIVO I	Sistema SAP / File Server
73	Patricia Herrera Cabanillas	JJC CONTRATISTAS GENERALES S.A.	FINANZAS	JEFE DE FINANZAS	Sistema SAP / Correo electrónico / File Server
78	Elizabeth Sánchez Joo	JJC CONTRATISTAS GENERALES S.A.	GERENCIA GENERAL	SECRETARIA DE GERENCIA	Correo electrónico
83	Eduardo Galloso Guerra	JJC CONTRATISTAS GENERALES S.A.	GESTION HUMANA	ADMINISTRADOR DE NOMINA III	Sistema SAP / File Server

Nro.	USUARIO	EMPRESA	ÁREA	CARGO	PRUEBA DE SERVICIO
92	José Zegarra Rodríguez	JJC CONTRATISTAS GENERALES S.A.	GESTION HUMANA	SUPERVISOR DE NOMINA	Sistema SAP / Correo electrónico / File Server
94	Luis Ugarte Centurión	JJC CONTRATISTAS GENERALES S.A.	GESTION HUMANA	SUPERVISOR DE ADMINISTRACION DE PERSONAL	Sistema SAP / Correo electrónico / File Server
96	Mauricio Martín Garma Rodríguez	JJC CONTRATISTAS GENERALES S.A.	GESTION HUMANA	GERENTE DE GESTIÓN HUMANA	Correo electrónico
101	Roberto Jauregui Linares	JJC CONTRATISTAS GENERALES S.A.	GESTION HUMANA	JEFE DE RECLUTAMIENTO Y SELECCION	Sistema SAP / File Server
129	Luis Valentine Díaz	JJC CONTRATISTAS GENERALES S.A.	INGENIERIA	JEFE DE PROYECTOS I	File Server
135	Miguel Silva Tica	JJC CONTRATISTAS GENERALES S.A.	INGENIERIA	JEFE DE PROYECTOS I	File Server
139	Raúl Moreano Mejía	JJC CONTRATISTAS GENERALES S.A.	INGENIERIA	GERENTE DE INGENIERÍA & PRESUPUESTO	Correo electrónico / File Server
142	Rolando Tala Romero	JJC CONTRATISTAS GENERALES S.A.	INGENIERIA	PROYECTISTA	Correo electrónico / File Server
149	Wilfredo Huamán Velásquez	JJC CONTRATISTAS GENERALES S.A.	INGENIERIA	ANALISTA DE PROPUESTAS II	Correo electrónico / File Server
150	Cesar Paz Orellana	JJC CONTRATISTAS GENERALES S.A.	LEGAL	ABOGADO II	Correo electrónico / File Server
156	Milagros Peña Portuondo	JJC CONTRATISTAS GENERALES S.A.	LEGAL	SECRETARIA DE GERENCIA	Correo electrónico / File Server
165	Hugo Pillaca Velásquez	JJC CONTRATISTAS GENERALES S.A.	LOGISTICA	ASISTENTE DE LOGISTICA II	Sistema SAP / File Server
167	José Antonio Ruiz Céspedes	JJC CONTRATISTAS GENERALES S.A.	LOGISTICA	JEFE DE LOGÍSTICA	Sistema SAP / File Server
173	Sixto Zapata Llontop	JJC CONTRATISTAS GENERALES S.A.	LOGISTICA	SUBGERENTE DE LOGÍSTICA	Sistema SAP / Correo electrónico / File Server
174	Trinidad Córdor Aguayo	JJC CONTRATISTAS GENERALES S.A.	LOGISTICA	JEFE SENIOR DE LOGISTICA	Sistema SAP / Correo electrónico / File Server
182	Juan Carlos Macciotta Urquiza	JJC CONTRATISTAS GENERALES S.A.	OPERACIONES	GERENTE INFRAESTRUCTURA Y EDIFICACIONES	Correo electrónico
187	Neil Molina Calle	JJC CONTRATISTAS GENERALES S.A.	OPERACIONES	GERENTE DE OFICINA TECNICA II	Correo electrónico / File Server
188	Paul Correa Rojas	JJC CONTRATISTAS GENERALES S.A.	OPERACIONES	ASISTENTE DE PROYECTOS II	Correo electrónico / File Server
191	Edgar Montoya Rojas	JJC CONTRATISTAS GENERALES S.A.	PLANEAMIENTO	ANALISTA DE CONTROL DE GESTION OP	Sistema SAP / File Server
193	Enrique Izaguirre Silva	JJC CONTRATISTAS GENERALES S.A.	PLANEAMIENTO	JEFE DE PLANEAMIENTO Y CONTROL DE GESTION	Sistema SAP / Correo electrónico / File Server
195	Alejandro Pineda Mayta	JJC CONTRATISTAS GENERALES S.A.	SEGUROS	JEFE GENERAL DE SEGUROS	Correo electrónico / File Server
196	Dan Joseph Campos Ortiz	JJC CONTRATISTAS GENERALES S.A.	SEGUROS	ASISTENTE DE SEGUROS	File Server
200	María Laura Quintanilla López	JJC CONTRATISTAS GENERALES S.A.	SERVICIOS Y SECRETARIA	SECRETARIA RECEPCIONISTA	Correo electrónico
238	Eduardo Távara García	JJC CONTRATISTAS GENERALES S.A.	UDE	JEFE DE EQUIPOS III	Correo electrónico / File Server
250	Gladys Porras Poma	JJC CONTRATISTAS GENERALES S.A.	UDE	ASISTENTE DE EQUIPOS II	Sistema SAP / File Server
262	Jimmy Ochoa Napa	JJC CONTRATISTAS GENERALES S.A.	UDE	ASISTENTE DE EQUIPOS II	Sistema SAP / Correo electrónico / File Server
287	Ricardo Montes Gómez	JJC CONTRATISTAS GENERALES S.A.	UDE	GERENTE DE EQUIPOS	Correo electrónico
312	Gustavo Jacobs Martínez	JJC EDIFICACIONES S.A.C.	EDIFICACIONES	GERENTE GENERAL	Correo electrónico
326	Millie Valdez Castañeda	JJC EDIFICACIONES S.A.C.	EDIFICACIONES	JEFE DE ADMINISTRACION DE VENTAS	Correo electrónico / File Server

Nro.	USUARIO	EMPRESA	ÁREA	CARGO	PRUEBA DE SERVICIO
328	Mónica Corrales Pérez	JJC EDIFICACIONES S.A.C.	EDIFICACIONES	ADMINISTRADOR	Correo electrónico / File Server
346	Enrique Acuña Pardo	JJC-SCHRADER CAMARGO S.A.C.	JJC-SC	GERENTE DE PROPUESTAS	Correo electrónico / File Server
349	Gustavo Peña Montoya	JJC-SCHRADER CAMARGO S.A.C.	JJC-SC	JEFE COMERCIAL	Correo electrónico / File Server
356	Patricia Miranda Mendoza	JJC-SCHRADER CAMARGO S.A.C.	JJC-SC	JEFE DE CONTABILIDAD	Sistema SAP / File Server

Fuente: Elaboración propia con información de JJC Contratistas Generales

En total se llevará a cabo la prueba de escritorio a 55 usuarios de la organización; excluyendo al equipo de TI (que son 7 personas) ya que ellos realizarán otro tipo de test.

Tabla 24

Cantidades de usuarios encuestados por cada área

ÁREA	CANTIDAD
ADMINISTRACION	2
ADMINISTRACION DE CONSORCIOS	2
ARCHIVO	2
AUDITORIA INTERNA	1
COMERCIAL	2
COMUNICACIONES	2
CONTABILIDAD	3
CSSM	3
EDIFICACIONES	3
FINANZAS	3
GERENCIA GENERAL	1
GESTION HUMANA	5
INGENIERIA	5
JJC-SC	3
LEGAL	2
LOGISTICA	4
OPERACIONES	3
PLANEAMIENTO	2
SEGUROS	2
SERVICIOS Y SECRETARIA	1
UDE	4
TOTAL GENERAL	55

Fuente: Elaboración propia

6.2 Revisión de resultados

En primer lugar, durante cada fase de la prueba se debe registrar la documentación detallada de las observaciones, problemas y las soluciones. La documentación actúa como importante información histórica que facilitará la recuperación real en caso de una paralización o desastre. Asimismo, la documentación contribuye a realizar un análisis detallado de las fortalezas y debilidades del plan de continuidad.

6.2.1 Análisis y evaluación de resultados

Es importante tener formas de medir el éxito del plan de continuidad y de las pruebas en función de los objetivos presentados al inicio. Por eso es importante que se midan los resultados cuantitativamente en vez de basarnos solamente en la observación.

Las mediciones varían según la prueba y la organización. Las buenas prácticas sugieren realizar las siguientes mediciones:

- Tiempo: El tiempo transcurrido para la terminación de las tareas definidas.
- Recuento: El número de servicios que se recuperaron con éxito.
- Cantidad: Cantidad de trabajo que el equipo de TI y los usuarios realizan en la ejecución del plan.
- Exactitud: La exactitud de la carga de datos en la sede de recuperación frente a la exactitud normal. También puede determinarse la exactitud de los ciclos de proceso reales comparando los resultados de salida con los del mismo período procesados en condiciones normales.

En el caso de nuestro proyecto, nos orientaremos más en mediciones de Tiempo ya que en los objetivos específicos se determinó definir tiempos óptimos que serán los aceptables por la organización para continuar con los servicios críticos.

En la siguiente tabla, vemos que todo el personal de TI conoce los procedimientos a seguir en caso de una paralización (sea para la prueba o escenario real), pero en categoría regular y buena. Lo mismo para los tiempos óptimos propuestos que compararemos más adelante.

Tabla 25

Respuestas del equipo de TI

RESULTADOS DE PRUEBAS DEL EQUIPO DE TI	RESPUESTAS
TECNOLOGIA DE LA INFORMACION	
PROCEDIMIENTO CORRECTO / TIEMPO OPTIMO	
Alexander Carlos Blanco Panduro - ADMINISTRADOR DE REDES Y COMUNIC. I	Regular / Buenas
Ángela María Carrasco Burneo - GERENTE TECNOLOGÍA DE INFORMACIÓN	Regular
Elvis Porras Poma - JEFE DE SOPORTE TECNOLÓGICO	Regular
Fernando Boza Gonzalez - JEFE SENIOR DE SERVICIOS TECNOLÓGICOS	Buenas
Geo Baccarani Rosas - JEFE DE SISTEMAS	Buenas
Reich Sánchez Torres - ADMINISTRADOR DE REDES Y COMUNIC. II	Buenas
Renzo Giancarlo Correa Salazar - ADMINISTRADOR DE REDES Y COMUNIC. I	Regular / Buenas
TOTAL GENERAL	7

Fuente: Elaboración propia

En la tabla 26, observamos las cantidades de respuestas categorizadas en “MUY BUENA”, “BUENA” y “REGULAR” para poder conocer si los usuarios conocen cómo seguir sus procesos de trabajo o qué hacer en caso no tengan activos sus servicios de TI. Aquí sabremos en dónde se tiene que reforzar el conocimiento del plan.

Tabla 26

Respuestas de usuarios por cada área evaluadas por el equipo de TI

RESULTADOS DE PRUEBAS DE USUARIOS	CANTIDADES
BUENA	26
ARCHIVO	1
AUDITORIA INTERNA	1
COMERCIAL	1

RESULTADOS DE PRUEBAS DE USUARIOS	CANTIDADES
CONTABILIDAD	2
EDIFICACIONES	2
GESTION HUMANA	2
INGENIERIA	3
JJC-SC	2
LEGAL	2
LOGISTICA	4
OPERACIONES	2
PLANEAMIENTO	2
UDE	2
MUY BUENA	17
ADMINISTRACION	1
ADMINISTRACION DE CONSORCIOS	1
CONTABILIDAD	1
CSSM	2
FINANZAS	3
GESTION HUMANA	3
INGENIERIA	2
JJC-SC	1
SEGUROS	1
UDE	2
REGULAR	12
ADMINISTRACION	1
ADMINISTRACION DE CONSORCIOS	1
ARCHIVO	1
COMERCIAL	1
COMUNICACIONES	2
CSSM	1
EDIFICACIONES	1
GERENCIA GENERAL	1
OPERACIONES	1
SEGUROS	1
SERVICIOS Y SECRETARIA	1
TOTAL GENERAL	55

Fuente: Elaboración propia

De las respuestas obtenidas de cada área sobre cada servicio y con las evidencias de las pruebas ejecutadas, ahora se mostrará los resultados finales de las pruebas de continuidad de los servicios críticos de la organización.

6.2.2 Evaluación de resultados – Equipo de TI

- Respuestas sobre procedimientos correctos a seguir y tiempos óptimos para las restauraciones de servicios:
 - Regular / Buenas: 2
 - Regular: 2
 - Buenas: 3

Nota: el resultado “Regular / Buenas” es considerado finalmente como “Regular”

Según los resultados de las pruebas de escritorio, vemos que hay algunas personas del equipo de TI que muestran un resultado regular. Como acción de mejora en este punto, se debe nuevamente repasar y reforzar procedimientos, correlación de acciones, ventanas de tiempo para las actividades, etc.

6.2.3 Evaluación de resultados – Usuarios de la organización

- Respuestas muy buenas: 17 usuarios
- Respuestas buenas: 26 usuarios
- Respuestas regulares: 12 usuarios

Según los resultados de las pruebas a los usuarios de la organización, se observa que hay un poco porcentaje de usuarios con respuestas regulares (22%), la mayoría da respuestas buenas (47%) y otra buena cantidad da respuestas muy buenas (31%).

Para el caso de los usuarios que presentaron respuestas regulares, se realizará nuevamente charlas de capacitación en todas sus áreas para poder reforzar el conocimiento de procedimientos a seguir en caso no cuenten con sus servicios críticos.

6.2.4 Evaluación de resultados (tiempos) – Servicios críticos de TI

- Servidores de archivos: 3 horas
- Sistema SAP: 5 horas
- Correo electrónico: 4 horas

Según los resultados de las pruebas de continuidad de los servicios críticos de TI, vemos que los tiempos de restauración de servicios están en un rango adecuado por la organización, ya que están no superan el tiempo máximo establecido por la empresa para estar sin servicios críticos de TI.

Además se debe tener en cuenta que los tiempos han sido determinados con cierta holgura para que sean cifras exactas (horas), ya que en la prueba real tomaron menos tiempo.

6.3 Validación de resultados

En puntos anteriores de este proyecto, se ha visto el cumplimiento de los objetivos específicos. El primer objetivo sobre “Identificar los riesgos de continuidad que podrían afectar los servicios críticos del área de Tecnología de la Información” dado que una parte fundamental e inicial del plan de continuidad es identificar los riesgos de continuidad, se demostró desde en el punto 4.1 al 4.3 y en la evaluación del riesgo en el punto 5.3.

Como se ve en la tabla 27; se identificaron todos los riesgos, pero se trabajó sobre los que tenían una valoración Muy Alta (MA) por acuerdo con la organización para poder primero tratar los que generarían un impacto grande. Estos riesgos se analizaron en diferentes

escenarios de amenaza y su probabilidad de ocurrencia junto con el impacto para poder presentar más adelante estrategias de continuidad con alternativas de solución.

Tabla 27

Resultado de identificación y evaluación del riesgo

TIPO DE AMENAZA	AMENAZA	PROBABILIDAD DE OCURRENCIA	IMPACTO	RIESGO
DESASTRES INDUSTRIALES	Corte de suministro eléctrico	M	MA	MA
	Problemas con el sistema de UPS	M	MA	MA
	Fallo de servicios de comunicaciones	M	MA	MA
ERRORES Y FALLOS NO INTENCIONADOS	Fallo en las copias de seguridad	M	MA	MA
	Destrucción de la información	M	MA	MA
	Caída del sistema por agotamiento de recursos	M	MA	MA
	Carencia de Alta Disponibilidad (HA)	M	MA	MA
ATAQUES INTENCIONADOS	Ataques por ingeniería social	B	MA	MA

Fuente: Elaboración propia

El segundo objetivo sobre “Desarrollar el análisis de impacto de negocio para poder determinar los impactos operacionales e impacto económico” se mostró en el punto 5.4.

En las tablas 28 y 29 se muestran los resúmenes tanto de la evaluación de impacto operacional como el económico respectivamente. En el operacional se obtuvo la estimación de horas de tolerancia a falla por cada servicio y en el económico a través de una fórmula determinada por

el negocio y por la gerencia de TI, se obtuvo la estimación de la pérdida económica para la empresa objetivo por hora y por día en el caso de paralización de los servicios.

Tabla 28

Impacto operacional de paralización de los tres servicios críticos

CATEGORÍA DEL SERVICIO	SERVICIO	NIVEL	TOLERANCIA A FALLAS (HORAS)	DESCRIPCIÓN
Aplicaciones	Sistema SAP	A	8	Sistema Principal de la empresa JJC Contratistas Generales S.A.
	Correo Electrónico	A	8	Servidor Exchange Server 2010 para Correo Electrónico
Sistemas de Almacenamiento	Servidores de Archivos	A	8	Servidores para guardar / compartir información

Fuente: Elaboración propia

Tabla 29

Impacto económico de paralización de los tres servicios críticos

SERVICIO	PÉRDIDA FIJA X SERVICIO (HORA)	HORAS DE CAÍDA	COSTO DE DETECCIÓN DE PROBLEMA Y RESTAURACIÓN DEL SERVICIO	TOTAL PÉRDIDA X DÍA
Sistema SAP	S/ 1,205.38	24	S/ 550.00	S/ 29,479.00
Correo Electrónico	S/ 741.88	24	S/ 350.00	S/ 18,155.00
Servidores de Archivos	S/ 993.75	24	S/ 350.00	S/ 24,200.00
			TOTAL	S/ 71,834.00

Fuente: Elaboración propia

El tercer objetivo sobre “Establecer estrategias de restauración y recuperación de los servicios críticos del área de TI”, también se demostró en el punto 5.5, donde se determinaron las diversas estrategias de continuidad para diferentes escenarios de paralización.

Tabla 30

Muestra de evaluaciones de estrategias de continuidad con alternativas de solución ante un escenario de paralización

TIPO DE AMENAZA	AMENAZA	RIESGO	ITEM	POSIBLE ESCENARIO DE FALLA DE LOS SERVICIOS	POSIBLE CAUSA DE FALLA DE LOS SERVICIOS	NRO DE ESTRATEGIA	ESTRATEGIA DE CONTINUIDAD	ALTERNATIVA DE SOLUCIÓN
ERRORES Y FALLOS NO INTENCIONADOS	<u>Carencia de Alta Disponibilidad (HA)</u>	MA	12	<u>Problema de réplicas entre servidores de archivos</u>	Mala configuración de las réplicas del servicio DFS	19	* Solicitar apoyo urgente al proveedor Corporación Sapia (según los SLA) para revisar configuración de réplicas * Buscar y restaurar la copia de información más cercana a la fecha de la última replicación	* Implementación y correcta configuración del servicio de replicación DFS y Name Space de Microsoft para la distribución de información entre File Servers del DC Principal y del DC Alterno) * Solicitar al proveedor custodio las cintas de Back-up para buscar información más cercana
			13	<u>Problema de réplicas del servidor de correo</u>	Mala configuración del servicio DAG para replicación de bases de datos	20	* Solicitar apoyo urgente al proveedor Corporación Sapia (según los SLA) para revisar configuración de réplicas * Buscar y restaurar la copia de información más cercana a la fecha de la última replicación	* Implementación y correcta configuración del servicio de replicación DAG de Exchange para la distribución de Bases de Datos de MailBox * Solicitar al proveedor custodio las cintas de Back-up para buscar información más cercana

Fuente: Elaboración propia

Por último, para el cuarto objetivo como se observa en la tabla 31, en la comparación de resultados finales, se valida la demostración del último objetivo específico de este proyecto que es: “Identificar y determinar periodos de recuperación requeridos por la organización para la continuidad de los servicios críticos del área de TI”.

Se analiza y compara los tiempos de restauración de servicios críticos de antes de la propuesta del diseño de plan continuidad junto con los propuestos después del diseño.

Tabla 31

Comparación de tiempos de restauración de los servicios críticos de TI

NRO.	SERVICIO CRÍTICO	TIEMPO TOLERABLE POR LA ORGANIZACIÓN	TIEMPO DE RESTAURACIÓN	
			ANTES	PROPUESTO Y PROMEDIADO EN PRUEBAS
1	SERVIDORES DE ARCHIVOS	24 horas	12 horas	3 horas
2	SISTEMA SAP	24 horas	18 horas	5 horas
3	CORREO ELECTRÓNICO	24 horas	12 horas	4 horas

Fuente: Elaboración propia

El tiempo de restauración considerado antes por la organización era entre 12 y 18 horas; pero ahora con el plan de continuidad planteado en este proyecto, se propone a la organización objetivo entre 3 a 5 horas en promedio para la restauración de los servicios críticos de TI basado en toda la elaboración del plan y con las pruebas reales ejecutadas donde se logra demostrar una mejora entre el 65% y 75% de menor tiempo para la recuperación de servicio en caso se presente una paralización.

7 CONCLUSIONES

Después de desarrollado el presente proyecto de diseño del plan de continuidad de servicios críticos de TI, se recopilan las siguientes conclusiones:

1. Se logró analizar la problemática que tenía la empresa y en base a ello, se realizó el diseño del plan de continuidad de servicios críticos de TI para mejorar los tiempos de recuperación y restauración.
2. En base a los resultados de los cuadros y matrices comparativas de realizar el análisis, evaluación y tratamiento de riesgos; el análisis de vulnerabilidades y amenazas; y el análisis de impacto de negocio, se logró identificar las estrategias de continuidad adecuadas con las alternativas de solución para proponer un buen diseño de plan que al final generará ahorro junto con mejoras en la operación y administración de los servicios críticos de TI.
3. Se logró realizar una prueba del plan de continuidad por cada servicio crítico de TI de la empresa objetivo con resultados satisfactorios (aceptados por la organización) con el fin de realizar la demostración de la mejora de los tiempos de recuperación y restauración.
4. Se logró evaluar cada área de la empresa (ejercicios de escritorio) para saber cómo pueden continuar sus procesos en caso se presente un caída parcial o total de los servicios críticos que utilizan según la labor que desempeñan. Con la mejora continua del plan, en un futuro se seguirán optimizando estos resultados.
5. Se logró los resultados esperados (reducción de tiempos de recuperación y restauración en 65% a 75%) por cada servicio crítico de TI en base a las alternativas de solución con alta disponibilidad para los servicios y los lineamientos de procedimientos mejorados y propuestos para el plan de continuidad.
6. Es muy importante que la gerencia general y la alta dirección se involucre en el proyecto ya que la implementación de un plan de continuidad de servicios críticos de TI es sólo un comienzo dentro de un largo camino de estabilidad y permanencia del negocio.

8 RECOMENDACIONES

El éxito de la puesta en marcha del plan de continuidad de servicios críticos de TI se dará cuando dicho plan sea concientizado y aprendido por todos los colaboradores de la empresa de un modo óptimo (tanto el personal de TI como los demás usuarios). Para ello se recomienda los siguientes puntos:

1. Seleccionar adecuadamente la infraestructura de hardware y software para soportar la continuidad de servicios de TI. Como se sabe, no siempre el producto más caro es sinónimo de ser el mejor, bajo ese concepto siempre será necesario realizar un cuadro comparativo con un análisis costo beneficio para seleccionar la infraestructura correcta con alta disponibilidad.
2. Realizar adecuadamente el análisis de riesgos, análisis de vulnerabilidades, análisis de amenazas, análisis de impacto de negocio y establecer las estrategias de continuidad siguiendo la norma ISO/IEC 27031:2011 y demás guías para la elaboración del diseño de plan.
3. Realizar pruebas periódicas para asegurarse del buen funcionamiento del plan de continuidad de servicios críticos de TI.
4. Documentar todas las fases de pruebas del plan con las observaciones, correcciones y mejoras de todas las novedades encontradas con el fin de aprovechar las lecciones aprendidas para incorporarlas en el plan de continuidad y que cumpla con su propósito de alcance de todos los resultados esperados.
5. Tomar también como referencia la norma ISO 22301:2012 que aportará un modelo general a la empresa objetivo para poder desarrollar el diseño del plan de continuidad que ha sido elaborado y descrito en este proyecto.
6. Que cada empresa en función de sus necesidades reales, diseñe, mantenga actualizado, probado y vigente su respectivo plan de continuidad de servicios críticos de TI, para que en caso de producirse uno o más escenarios de paralización tengan una ventaja competitiva al convertir las pérdidas en ganancias, utilizando la mejora continua del plan mediante opciones de inversión que aseguren la continuidad de dichos servicios y que además incrementen la capacidad, disponibilidad y rendimiento de los recursos empresariales.

9 REFERENCIAS

BRAVO ESTRADA, Diego (2010) Recomendaciones de seguridad en sistemas distribuidos de cómputo (V0.11) (consulta 01 de setiembre de 2018) (<http://es.tldp.org/Tutoriales/doc-tutorial-recomendaciones-seguridad/doc-tutorial-recomendaciones-seguridad.pdf>)

COBO, Juan Cristóbal (2009) El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento, pp. 295 – 318 En: Revista de Estudios de Comunicación, vol. 14, no. 27.

COLLAZOS BRAHAM, José David (2012) Plan de contingencia basado en alta disponibilidad y virtualización (tesis de Ingeniería de Sistemas). Pereira: Universidad Tecnológica de Pereira.

FILIPPI, Carlos y SERAFINI Emilse (2012) Caso de Éxito: Implementación del Marco de Trabajo de Continuidad de la Infraestructura de TI de ARANDU. En: Segunda Conferencia de Directores de Tecnologías de Información y Comunicación de Instituciones de Educación Superior. Asunción: UNA

GARAY, José (2012) Antecedentes Históricos de la Continuidad del Negocio (consulta: 01 de setiembre de 2018) (<http://businesscontinuity-pe.blogspot.pe/2012/07/antecedentes-historicos-de-la.html>)

GÓMEZ, Álvaro y SUÁREZ, Carlos (2011) Sistemas de Información, Herramientas prácticas para la gestión empresarial. Vigo: Ra-Ma

INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA (INEI) (2001) Guía práctica para el desarrollo de planes de contingencia de sistemas de información. Lima: INEI.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) (2011) Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity. ISO/IEC 27031:2011. Traducción propia.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) (2012) Sistema de Continuidad de Negocio. ISO/IEC 22301:2012.

JJC CONTRATISTAS GENERALES S.A (2016) (<http://www.grupojjc.com.pe/>) Sitio Web oficial de JJC; contiene información sobre la institución y enlaces de interés. (consulta: 01 de setiembre de 2018)

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (MINTIC) (2015) Guía para realizar el Análisis de Impacto de Negocios BIA. Bogotá: MINTIC

MONTERO GONZALEZ, Fernando Enrique (2011) Gestión del riesgo en infraestructura y comunicaciones TI, para empresa del sector financiero (tesis de Ingeniería Civil Telemática). Valparaíso: Universidad Técnica Federico Santa María.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (2010) Contingency Planning Guide for Federal Information Systems. Gaithersburg: NIST Department of Commerce. Traducción propia.

OCHOA CEBALLOS, Marco Antonio (2015) Plan de continuidad de los servicios críticos de red de la empresa Actuaría Consultores cía. Ltda. Fundamentado en los estándares internacionales de Cobit, ITIL e ISO 20000 (tesis de Máster en Redes de Comunicaciones). Quito: Pontificia Universidad Católica del Ecuador.

RUGGIRELLO, Hernán (2011) El sector de la construcción en perspectiva. Internalización e impacto en el mercado de trabajo. Buenos Aires: Aulas y Andamios.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER (UFPS) (2015) Plan de contingencia de TI. Ocaña: UFPS.

10 GLOSARIO

Ancho de Banda: longitud medida en hertzios (Hz), de la extensión de frecuencias en la que se concentra la mayor potencia de la señal.

Amenaza: hecho que puede producir un daño provocado por un evento.

Back-up: copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Caída de enlace y/o servicio: declinación o declive del enlace, sea de conexión de algún sistema, de datos o de Internet.

Centro de Datos: ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

Contingencia: suceso que puede ocurrir o no, especialmente un problema que se plantea de forma imprevista.

Continuidad: circunstancia de tener un servicio sin interrupción.

Disponibilidad: posibilidad de tener un servicio activo cuando se necesite.

File Server: servidor que brinda el servicio de almacenar y compartir archivos.

Hosting: servicio de alojamiento externo.

Housing: servicio que consiste en tener un espacio físico en un lugar externo.

Malware: código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

Metrado: cuantificación detallada por partidas de las actividades por ejecutar o ejecutadas en una obra.

Nube: es un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.

Paralización: detención (paro) que experimenta un servicio que está en actividad.

Recuperación: tener activo nuevamente un servicio en el tiempo más pronto posible para que los usuarios continúen sus procesos.

Restauración: reactivación del servicio de modo total a como estaba antes. Servicio que se brinda para obtener información desde una copia de seguridad almacenada.

Red Privada Virtual: servicio que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.

Replicación: proceso mediante el cual se genera una copia exacta de parte del sistema y puede ser desde un archivo hasta una carpeta, una partición, un disco o incluso varios discos.

Riesgo: medida de la magnitud de los daños frente a una situación peligrosa.

Saturación: Llenar u ocupar un servicio hasta el límite de su capacidad.

Sistema ERP: Sistema integrado de gestión compuesto por un conjunto de módulos funcionales que son adaptados a las necesidades de cada cliente.

11 SIGLARIO

BIA:	Business Impact Analysis
ERP:	Enterprise Resource Planning
HA:	High Availability
IP:	Internet Protocol
ISO:	International Organization for Standarization
ISP:	Internet Service Provider
TI:	Tecnología de la Información
TIC:	Tecnología de la Información y la Comunicación
VPN:	Virtual Private Network
SGSI:	Sistema de Gestión de Seguridad de la Información
PDCA:	Plan, Do, Check, Act
iRBC:	Information Communication Technology Readiness for Business Continuity
NIST:	National Institute of Standards and Technology
INEI:	Instituto Nacional de Estadística e Informática
RTO:	Recovery Time Objective
RPO:	Recovery Point Objective
MBCO:	Minimum Business Continuity Objective

12 ANEXOS

Anexo 1. Matriz de probabilidad e impacto referente a los riesgos.

MA: Muy Alto

A: Alto

M: Medio

B: Bajo

MB: Muy Bajo

<i>riesgo</i>		<i>probabilidad</i>				
		MB	B	M	A	MA
<i>impacto</i>	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Elaboración propia

Esta matriz servirá para poder catalogar los riesgos según su probabilidad de ocurrencia y su impacto en los servicios críticos de la empresa. Ayudará de manera más sencilla a definir el nivel de riesgo que tiene cada servicio para luego poder realizar el análisis necesario que involucra el plan de continuidad.