UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERIA

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

**Diseño de un Plan de Recuperación de Desastres de TI (DRP TI) para el
Centro de Cómputo de la sede principal de una entidad educativa superior del
sector privado basado en la norma NIST SP 800-34**

TESIS

Para optar el título profesional de Ingeniero de Redes y Comunicaciones

AUTOR(ES)

Yarlequé Gutiérrez, Alfredo (0000-0002-9449-2012)

ASESOR

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

Lima, 02 de abril de 2019

DEDICATORIA

Dedico la presente tesis a mis padres por su esfuerzo para darme educación, que de alguna manera este triunfo pueda recompensar ese sacrificio, valores y sostén para seguir adelante en los momentos más difíciles.

De igual manera, dedico esta tesis a mi esposa quien siempre me aconsejó y creyó en mí desde que empecé este difícil camino para lograr obtener el título profesional de ingeniero.

A mis amigos y compañeros de trabajo que con sus conocimientos y experiencias aportaron en mi desarrollo profesional y también personal.

A la facultad de ingeniería de la UPC por brindarme los conocimientos necesarios para desarrollarme como ingeniero y a mi asesor por sus consejos y recomendaciones en todo momento.

RESUMEN

El presente trabajo constituye un documento de apoyo dentro de una entidad educativa superior del sector privado para la elaboración de su Plan de Recuperación de Desastres de TI para salvaguardar el bien máspreciado de la organización que es la información. El tema de la presente tesis se desarrolla entorno al diseño de un DRP de TI alineado a los procesos y servicios que posee y que permita contribuir con el logro de los objetivos institucionales. El presente documento está dividido en cinco capítulos. En el primero, se desarrolla el plan de tesis, donde se explica la problemática, la motivación y otros aspectos introductorios que determinaron el desarrollo del presente proyecto. En el segundo capítulo, se desarrolla el marco teórico, que permitirá brindar conocimiento al lector sobre todos los temas relevantes y relacionados a este documento como es el DRP de TI, diferentes normas internacionales lo sindicand de diferentes maneras. En el tercer capítulo, se desarrolla la definición del problema, donde se establece el alcance, se realiza el Análisis de Riesgos identificando los escenarios de amenazas y la elaboración del Análisis de Impacto de Negocio. En el cuarto capítulo se desarrolla el diseño de la solución, se establece la política y estructura organizacional que evaluará la situación de contingencia o indisponibilidad según sea el escenario, además se implantan los lineamientos para su elaboración. Finalmente en el quinto capítulo, se desarrolla las pruebas, resultados y validaciones, donde se muestra el plan de pruebas, actividades de notificación, evaluación y activación.

Palabras clave: DRP TI; Plan de Recuperación de Desastres; Análisis de impacto de negocio; Análisis de Riesgos; contingencia.

Design of an IT Disaster Recovery Plan (IT DRP) for the Computing Center of the
headquarter of a higher education private sector entity based on the NIST SP 800-34
standard

ABSTRACT

The present work constitutes a support document within a higher education entity of the private sector for the preparation of its IT Disaster Recovery Plan to safeguard the most precious asset of the organization, which is information. The theme of this thesis is developed around the design of an IT DRP aligned to the processes and services that it has and that allows contributing to the achievement of institutional objectives. This document is divided into five chapters. In the first, the thesis plan is developed, where the problem, motivation and other introductory aspects that determined the development of the present project are explained. In the second chapter, the theoretical framework is developed, which will provide knowledge to the reader on all relevant issues and related to this document as it is the IT DRP, different international standards syndicate it in different ways. In the third chapter, the definition of the problem is developed, where the scope is established, the Risk Analysis is carried out, identifying the threat scenarios and preparing the Business Impact Analysis. In the fourth chapter, the design of the solution is developed, the policy and organizational structure is established, which will evaluate the contingency or unavailability situation according to the scenario, and the guidelines for its preparation are also implemented. Finally, in the fifth chapter, the tests, results and validations are developed, where the test plan, notification, evaluation and activation activities are shown.

Keywords: DRP TI; Disaster Recovery Plan; Business impact analysis; Risk analysis; contingency.

TABLA DE CONTENIDOS

1	ASPECTOS INTRODUCTORIOS.....	1
1.1	ORGANIZACIÓN OBJETIVO.....	1
1.2	CAMPO DE ACCIÓN EN LA ORGANIZACIÓN	1
1.3	SITUACIÓN PROBLEMÁTICA	2
1.4	IDENTIFICACIÓN DEL PROBLEMA	2
1.5	OBJETIVOS.....	2
1.5.1	Objetivo General.....	2
1.5.2	Objetivo específico	3
1.6	INDICADORES O MECANISMOS DEL LOGRO DE LOS OBJETIVOS	3
1.7	JUSTIFICACIÓN DEL PROYECTO	4
1.8	ESTADO DEL ARTE	4
2	MARCO TEORICO.....	13
2.1	CONCEPTOS GENERALES	13
2.2	CONCEPTOS RELACIONADOS A LA RECUPERACIÓN DE DESASTRES DE TI	18
2.3	MARCO REGULATORIO LEGAL	29
2.4	METODOLOGÍAS	31
3	DEFINICION DEL PROBLEMA	38
3.1	ALCANCE DE DRP	38
3.2	ANÁLISIS DE RIESGOS DE CONTINUIDAD DE DRP.....	38
3.3	DISEÑO DEL ANÁLISIS DE IMPACTO DE NEGOCIO.....	42
3.4	ELABORACIÓN DE BIA	46
3.5	ESTRUCTURA DE DESGLOSE DE TRABAJO	52
3.6	ESTRATEGIAS DE DRP	52
3.7	MATRIZ DE ESTRATEGIAS	55
4	DISEÑO DE LA SOLUCION	59
4.1	DECLARACIÓN DE POLÍTICA DE CONTINUIDAD DE NEGOCIO.....	59
4.2	ELABORACIÓN DE DRP	60
4.3	EJECUCION DEL PLAN DE RECUPERACION	73
5	PRUEBAS, RESULTADOS Y VALIDACION	85

5.1	RESULTADO DE INDICADOR DE LOGRO 1	86
5.2	RESULTADO DE INDICADOR DE LOGRO 2.....	87
5.3	RESULTADO DE INDICADOR DE LOGRO 3	89
5.4	RESULTADO DE INDICADOR DE LOGRO 4.....	89
5.5	PLAN DE PRUEBAS DE DRP	90
5.6	VALIDACIÓN DE EJECUCIÓN DEL PLAN	95
6	REFERENCIAS	115
7.	ANEXOS	122

ÍNDICE DE TABLAS

Tabla 1 Sistema de información de recursos, tabla de componentes	37
Tabla 2 Escenarios de riesgos.....	39
Tabla 3 Leyenda de probabilidad	40
Tabla 4 Leyenda de impacto.....	41
Tabla 5 Clasificación y valoración de los riesgos	41
Tabla 6 Mapa de Riesgos.....	42
Tabla 7 Cuestionario aplicado al proceso de Matricula	44
Tabla 8 Listado de áreas de negocio.....	46
Tabla 9 Factores considerados para evaluar el impacto	47
Tabla 10 Clasificación de los procesos evaluados.....	47
Tabla 11 Mapa de procesos de la organización	48
Tabla 12 Listado de procesos evaluados	48
Tabla 13 Sub procesos con criticidad alta	50
Tabla 14 Sub procesos con criticidad media	50
Tabla 15 Sub procesos con criticidad baja	51
Tabla 16 Matriz de Estrategias	55
Tabla 17 Matriz de alternativas de solución por estrategia	56
Tabla 18 Resumen de objetivos específicos y requerimientos	57
Tabla 19 Miembros de cada grupo de recuperación.....	61
Tabla 20 Escenarios de Desastres en la sala de servidores.....	74
Tabla 21 Prioridad de recuperación 0.....	74
Tabla 22 Prioridades de Recuperación 1	75
Tabla 23 Prioridades de Recuperación 2	75
Tabla 24 Prioridades de Recuperación 3	75
Tabla 25 Ubicación de sitio alternativo.....	76
Tabla 26 Equipos necesarios para la contingencia	77
Tabla 27 Componentes necesarios para la contingencia	77
Tabla 28 Identificación de prefijos por equipos	78
Tabla 29 Descripción de los campos de las tablas de actividades.....	79
Tabla 30 Declaración de contingencia.....	80
Tabla 31 Activación de equipos de trabajo	81
Tabla 32 Bitácora de cambios	84

Tabla 33 Relación de cada logro con el objetivo específico	85
Tabla 34 Matriz de riesgos	86
Tabla 35 Mapa de riesgo	87
Tabla 36 Sub procesos con criticidad Alta	87
Tabla 37 Sub procesos con criticidad media	88
Tabla 38 Sub procesos con criticidad baja	88
Tabla 39 Matriz de estrategias.....	89
Tabla 40 Matriz de alternativas de solución por estrategias.....	89
Tabla 41 Escenario de Plan de Pruebas	91

ÍNDICE DE FIGURAS

Figura 1. Ciclo de vida del BCM.....	6
Figura 2. Fases del modelo PDCA	9
Figura 3. Disaster Recovery vs. Business Continuity	10
Figura 4. Tipos de Amenazas de Continuidad.....	14
Figura 5. Tipos de Riesgos	15
Figura 6. Matriz de riesgos en un análisis cualitativo de impacto y probabilidad	17
Figura 7. Tipos de Controles	18
Figura 8. Matriz de relación entre la ISO 27001 y la ISO 22301	21
Figura 9. Principios de COBIT	22
Figura 10. Marco de trabajo para la gestión de riesgos	32
Figura 11. Gestión de Riesgos	32
Figura 12. Proceso de gestión de riesgos.....	33
Figura 13. Proceso BIA	34
Figura 14. Balance de costo.....	36
Figura 15. Clasificación de los Sub-Procesos	51
Figura 16. Estrategias de continuidad y recuperación costo vs. Tiempo	55
Figura 17. Estructura Organizacional de DRP	60
Figura 18. Procedimiento de respuesta a la contingencia.....	78
Figura 19. Diagrama de proceso de control de cambios	83
Figura 20. Clasificación de los Sub-procesos.....	88
Figura 21. Plan de pruebas 2019	95

1 ASPECTOS INTRODUCTORIOS

1.1 Organización Objetivo

La organización beneficiada es una entidad educativa superior del sector privado la cual brinda servicios educativos desde el año 1994 y pertenece a una red internacional de universidades, para brindar oportunidad a los alumnos de estudiar en instituciones superiores de excelencia de todo el mundo y formar profesionales preparados a nivel internacional. En el año 2012 se inició las clases descentralizadas de Pregrado en uno de sus Campus y en el año 2013 se unió el otro Campus. En ese mismo año se inauguró una nueva sede mediante la cual afianza su sistema educativo. La misión de esta universidad es “Formar líderes íntegros e innovadores con una visión global para que transformen al Perú” y tiene como visión “Ser líder en la educación superior por su excelencia académica y su capacidad de innovación”.

La universidad cuenta con 1860 usuarios administrativos aproximadamente distribuidos en los diferentes campus ubicados en la ciudad de Lima. El trabajo diario del personal administrativo soporta el núcleo del negocio de la organización y se apoya en los sistemas de información que crecen día a día. Asimismo, los sistemas de información son soportados por las herramientas informáticas como servidores, software, infraestructura de red y los mismos se alojan en los centros de cómputo de las principales sedes de la universidad. Los servidores como principales medios de almacenamiento se respaldan en un arreglo de discos duros, para luego ser copiados a cintas magnéticas, las cuales se custodian en las sedes diferentes.

1.2 Campo de acción en la organización

El campo de acción en la entidad educativa superior del sector privado será el área de Infraestructura, Plataforma y Cloud que pertenece a la Gerencia de TI y a la Dirección de Innovación y Transformación, la cual se encarga de la administración de la infraestructura y plataforma de servidores y servicios informáticos que se encuentran alojados en el centro de cómputo ubicado en la sede principal, entre esos se tiene los principales sistemas que soporta el núcleo de negocio de la organización.

Está área es la responsable del proceso de respaldo y restauración de los sistemas de información que soporta; así como, el área de Redes y Telecomunicaciones tiene la administración de las redes de datos y los servicios de voz de la misma.

1.3 Situación problemática

La entidad educativa superior del sector privado tiene políticas y procedimientos establecidos de respaldo y restauración de la información de sus sistemas y pertenecen al área de Infraestructura, Plataforma y Cloud, estas políticas y procedimientos contemplan la ejecución, con frecuencia trimestral, de pruebas de restauración de información, si bien se tienen estas actividades calendarizadas, ante un eventual desastre que afecte los servicios informáticos que se encuentran en el centro de cómputo de la sede principal, no se tiene un documento guía del orden de ejecución de las actividades de recuperación, no solo se debe definir la pronta recuperación de los servidores y servicios, sino establecer la sincronía con la habilitación de los componentes de comunicación interna y externa, así como los proveedores de energía eléctrica; por ello tendrá impacto en los principales procesos de gestión y marketing de esta universidad; siendo así, la organización no se encuentra preparada para afrontar un desastre o evento que pudiese paralizar las actividades operacionales de los sistemas de información del centro de cómputo de la sede principal; los cuales pueden causar cuantiosas pérdidas a la universidad, como el impacto irremediable en su imagen y prestigio.

1.4 Identificación del problema

Debido a la creciente dependencia que presenta esta entidad educativa superior del sector privado sobre sus tecnologías de información como soporte a sus procesos críticos de negocio y si bien, la organización cuenta con procesos de respaldo y restauración de información, incluyendo pruebas de restauración de información con frecuencia trimestral y restauración de los principales sistemas de manera anual, no se encuentra documentado los procedimientos y acciones a seguir cuando se presente un inminente desastre, ya sea causado por la naturaleza o por la mano del hombre. Además de ello, la organización no se encuentra preparada para afrontar de manera eficaz y efectiva esa situación.

1.5 Objetivos

1.5.1 Objetivo General

Diseñar un Plan de Recuperación de Desastres de TI (DRP TI) basado en la norma internacional NIST SP 800-34 Guía de Planificación de Contingencia para Los Sistemas de

Información, que permita establecer las acciones y mecanismos requeridos que puedan garantizar la continuidad operativa del centro de cómputo de la sede principal de la universidad

1.5.2 Objetivo específico

Realizar un Análisis de Riesgos que permita determinar los escenarios de amenazas que podrían afectar al centro de cómputo.

Desarrollar un Análisis de Impacto al Negocio (BIA), que permita determinar el impacto operacional y económico, que podría tener la universidad como resultado de la ocurrencia de una interrupción o desastre.

Definir las estrategias de recuperación de desastres de TI que permitirán cumplir con los objetivos de recuperación establecidos por el centro de cómputo.

Definir las alternativas de solución de recuperación para las estrategias.

1.6 Indicadores o mecanismos del logro de los objetivos

Objetivo Específico	Indicador de Logro	Métrica
Realizar un Análisis de Riesgos que permita determinar los escenarios de amenazas que podrían afectar al centro de cómputo.	Informe de Análisis de Riesgos Matriz de riesgos.	Escenarios de amenazas críticos o más relevantes. Amenazas de mayor probabilidad de ocurrencia
Desarrollar un Análisis de Impacto al Negocio (BIA), que permita determinar el impacto operacional, económico, que podría tener la universidad como resultado de la ocurrencia de una interrupción o desastre.	Informe de Análisis de Impacto de Negocio (BIA). <ul style="list-style-type: none"> - Niveles de Servicio - Recursos Críticos - Prioridades de Recuperación - Procesos y Servicios Críticos 	Nivel de RPO, RTO y MTPD. Nivel de criticidad de los recursos críticos. Prioridades de recuperación. Nivel de criticidad de procesos y servicios.
Definir las estrategias de recuperación de desastres de TI que permitirán cumplir con los objetivos	Matriz de estrategias.	Cantidad de Estrategias (N°) - Tiempo

de recuperación establecidos por el centro de cómputo.		- Calidad
Definir las alternativas de solución de recuperación para cada estrategia.	Matriz de Alternativas de Solución.	Cantidad de Alternativas de Solución (N°) - Proveedores

1.7 Justificación del proyecto

Por ser un riesgo latente el no estar preparados ante desastres o eventos que pudiesen acontecer con la posterior paralización de las operaciones de la entidad educativa y la inactividad del soporte tecnológico que brinda el centro de cómputo de la sede principal a los procesos críticos de negocio, es necesario establecer los procedimientos y acciones para que se alinee a un Plan de Recuperación de Desastres de TI basado en la norma NIST SP 800-34, con la finalidad de mantener la continuidad de los servicios relacionados a los sistema de información, protegiendo al negocio de fallas generales en los servicios informáticos y minimizando el riesgo generado por la falta de estos servicios, garantizando el acceso a la información, disminuyendo la toma de decisión errónea de presentarse algún desastre y tener la capacidad de recuperación exitosa; así como mitigar el impacto económico negativo ante una situación adversa, brindando condiciones para continuar la operación del centro de cómputo, haciendo más competitiva y eficiente a la universidad.

1.8 Estado del arte

BCM (Business Continuity Management)

La Gestión de la Continuidad del Negocio es un proceso holístico que identifica amenazas potenciales a la organización e impactos a las operaciones del negocio que tales amenazas puedan causar en caso de materializarse; y proporciona la estructura para construir resiliencia con capacidad para dar respuesta efectiva protegiendo los intereses de las partes interesadas, el valor de la marca, la reputación y las actividades creadoras de valor.

- Asignación de responsabilidades: Un programa de BCM exitoso depende de la identificación de roles y responsabilidades y autoridad claramente definidos para

manejo del BCM y su proceso a través de la organización. El propósito de la asignación de roles y responsabilidades es garantizar que el personal comprenda sus funciones y responsabilidades y asegurar que las tareas requeridas para el mantenimiento del BCM están asignadas a individuos competentes cuyo desempeño pueda monitorearse.

- Mantenimiento de BCM en la organización: El mantenimiento del BCM involucra la gestión de un número de proyectos relacionados y la coordinación de las actividades que lo equilibra:
 - Sensibilización: Eventos que mantienen el entusiasmo para llevar a cabo el BCM.
 - Planificación: Desarrollo de planes para responder a los incidentes que pudieran no ocurrir.
 - Medidas de Mitigación: Implementación de medidas para mitigar el impacto de un incidente que pueda ocurrir mientras el programa está siendo desarrollado.
 - Ejercicio: Ejercicios para practicar los planes de contingencia.

El propósito de este paso es asegurar que se mantiene un BCM sostenible en la organización. Al decir sostenible, es que se ha ganado el compromiso de la organización y cuenta con estructura y procedimientos en sitio para asegurar que está mantenido y mejorado y está disponible para el futuro previsible.

- Gestión del Proyecto: Cuando se compromete al mantenimiento del BCM en una organización se deben adoptar las disciplinas de Gestión de Proyectos. Los métodos seleccionados de Gestión de Proyectos deben ser adecuados al tamaño y complejidad de la organización.
- Gestión continua de la Continuidad del Negocio: El BCM necesita gestionarse en un ciclo continuo de mejora para su eficacia. Esto involucra la participación de varias áreas gerenciales, operativas, administrativas y técnicas que necesitan estar coordinadas.

- Documentación del BCM: Una parte importante del BCM es la gestión de su documentación, la cual necesita llevarse a cabo de una manera que sea consistente y fácil de entender. El nivel y tipo de documentación debe ser apropiado al tipo y tamaño de la organización.

Elementos del Ciclo de Vida del BCM

Lo conforman un conjunto de actividades de la Continuidad del Negocio que colectivamente cubren todos los aspectos y fases del BCM, que se repite como objetivo general de mejorar la resiliencia organizacional. Se divide en seis prácticas profesionales:

Figura 1. Ciclo de vida del BCM

BCI 2013

Prácticas de Gestión

a) Política y Gestión de Programas

Es el inicio del ciclo de vida del BCM y se trata de la práctica profesional que define la política de la organización y la forma en que la política se llevará a cabo, controladas y validadas a través de un programa de BCM. La política BC incluye: La definición de BC para la organización y del ámbito de aplicación del BCM, asignar roles y responsabilidades de BC; un framework para la gestión del BCM; un conjunto de principios, directrices y

estándares mínimos; una definición clara de presupuesto, auditoría y responsabilidades de gobernanza.

b) Incorporación de Continuidad de Negocio

Es la práctica profesional que continuamente busca integrar BC en las actividades empresariales del día a día y la cultura organizacional. Esta actividad no es exclusiva de BC; otras disciplinas también deben incorporarse en la organización de una manera similar. Disciplinas como la Calidad, Salud y Seguridad, Servicios Ambientales, Seguridad y Gestión de Riesgos tiene retos similares. Así que la oportunidad de compartir experiencias y oportunidades de aprendizaje a través de diversas disciplinas relacionadas es importante.

Prácticas Técnicas

c) Análisis

Es la práctica profesional dentro del ciclo de vida de BCM que revisa y evalúa una organización en términos de cuáles son sus objetivos, su funcionamiento y las limitaciones del entorno en el que opera. La información recogida permite determinar la mejor manera de preparar una organización para ser capaz de manejar las interrupciones que de otro modo podrían seriamente o fatalmente dañarlo.

La principal técnica utilizada para el análisis de una organización para la continuidad del negocio (BC) es el análisis del impacto del negocio (BIA). A nivel estratégico, puede hacer preguntas a la Alta Dirección que se refieren a la misión de la organización, sus objetivos, los objetivos y las prioridades. También se pueden utilizar los niveles táctico y operacional para profundizar e identificar información más detallada.

Esta práctica profesional cubrirá la estimación de los recursos, instalaciones y servicios externos que requerirá cada actividad, tanto en la reanudación y volver a las operaciones normales. Dentro del programa de BCM, esta etapa debe centrarse en las amenazas inherentes a las actividades de negocios identificados como más urgentes en el BIA, en lugar de todas las amenazas a la organización.

d) Diseño

Es la práctica profesional dentro del ciclo de vida de BCM que identifica y selecciona las estrategias y tácticas para determinar la continuidad y recuperación de las pérdidas que se

lograrán. La información obtenida de la etapa de análisis y decisiones tomadas en la etapa de Políticas y Gestión de Programas se utilizan para diseñar soluciones en las siguientes tres áreas:

- Continuidad y estrategias de recuperación y tácticas
- Medidas de mitigación de amenazas
- Estructura de respuesta a incidentes

e) Implementación

Es la práctica profesional dentro del ciclo de vida del BCM que ejecuta las estrategias acordadas y tácticas a través del proceso de elaboración del Plan de Continuidad de Negocios (BCP). El objetivo es identificar y documentar las prioridades, procedimientos, responsabilidades y recursos para ayudar a la organización en la gestión de un incidente perturbador, mientras que la aplicación de estrategias de continuidad y recuperación a un nivel predeterminado de servicio.

f) Validación

Es la práctica profesional dentro del ciclo de vida de BCM que confirma que el Programa de BCM responde a los objetivos establecidos en la Política de BC y que el BCP de la organización es apto para el propósito. El objetivo de la validación es garantizar que la capacidad BC refleja la naturaleza, escala y complejidad de la organización que apoya y que es actual, precisa y completa, y que se adopten medidas para mejorar continuamente la resiliencia organizacional.

PDCA (Plan, Do, Check, Act)

Es un modelo para la planificación, establecimiento, implementación, operación, supervisión, revisión y mantenimiento de la mejora continua de la eficacia de un BCMS de la organización. Las fases del modelo Planificación- Implementación- Verificación- Mantenimiento son:

Figura 2. Fases del modelo PDCA

BSI 2012

Plan (Establecer): Establecer la política, objetivos, controles, procesos y procedimientos de continuidad de negocio con el fin de obtener resultados que se alinean con las políticas generales y los objetivos de la organización.

Do (Implementar y Operar): Implementar y operar la política de la continuidad de negocios, controles proceso y procedimientos.

Check (Monitorear y Revisar): Monitorear y evaluar el desempeño de la política de continuidad de negocio y los objetivos, informando de los resultados a la gerencia para su revisión, y determinar y autorizar las acciones de remediación y mejoramiento.

Act (Mantener y Mejorar): Mantener y mejorar los BCMS mediante la adopción de medidas correctivas, con base en los resultados de la revisión de la gestión y la revalorización del alcance de las BCMS y la política y objetivo de continuidad de negocio.

En la actualidad las organizaciones deben evaluar y tomar las medidas para que la información se mantenga íntegra, debido a los acontecimientos que vulneran este aspecto (desastres naturales, ataques cibernéticos, guerras, etc.) se debe considerar que el Plan de Continuidad de Negocios y un Plan de Recuperación de Desastres - DRP TI, aun cuando son de vital importancia para la contingencia no son lo mismo. Cuando se evalúa la posibilidad de ocurrencia de un desastre o tener alguna contingencia, las organizaciones suelen confundir estos planes o en el mejor de los casos, utilizan los términos de manera ambigua,

como si fueran lo mismo. La principal diferencia se encuentra en su alcance, ya que el BCP son acciones que garantizan que las operaciones continúen a pesar de una contingencia, recuperando los procesos críticos para ello; mientras que el DRP se encarga sólo de la recuperación y restablecimiento de los procesos de infraestructura TI; es por ello, que el DRP se encuentra contemplado dentro del BCP. Entonces, ambos son necesarios y favorecen a los sistemas esenciales para el correcto funcionamiento del negocio cuando sea requerido.

Figura 3. Disaster Recovery vs. Business Continuity

Matt Sprague: Manager of Infrastructure Services, CDI Manager Services

INSTITUCIONES

Business Continuity Institute (BCI)

El BCI fue establecido en 1994 para permitir a los miembros obtener orientación y apoyo de los compañeros practicantes de continuidad del negocio. El rol más amplio de la BCI es promover los más altos estándares de competencia profesional y ética comercial en la provisión y mantenimiento de la planificación de la continuidad del negocio y Servicios.

Los objetivos principales del BCI consiste en:

- Establecer, mantener y promover altos estándares para la práctica ética de BCM, incluyendo entrega de bienes y servicios.

- Establecer y fomentar una educación de calidad y el desarrollo personal de los practicantes de todos los niveles.
- Para iniciar, desarrollar, evaluar y comunicar el pensamiento BCM, estándares y buenas prácticas.
- Para influir en los responsables políticos, líderes de opinión y otros grupos de interés en todo el mundo en el tema de BCM.

Disaster Recovery Institute International (DRI)

DRI International es una organización sin fines de lucro fundada en 1988 como el Instituto de Recuperación de Desastres para lograr que profesionales de diversas industrias y sectores empresariales entiendan los principios de continuidad de negocio y mantengan su nivel de conocimiento a través de una educación continua. DRI Internacional tiene como objetivo promover base de conocimiento para la continuidad del negocio y la recuperación de desastres. Esto lo logran a través de la educación, la asistencia y la publicación de la base de recursos estándar. Por otro lado, administra los principales programas de certificación para las personas comprometidas en la práctica y gestión de continuidad de negocios.

Sus objetivos son:

- Promover una base común de gestión de la continuidad de la profesión.
- Promover la credibilidad y la profesionalidad de las personas certificadas.
- Lograr que los certificados tengan claro el tema de recuperación de desastres.

National Institute of Standards and Technology (NIST)

El Instituto Nacional de Estándares y Tecnología (NIST) es un organismo federal no regulador que forma parte de la Administración de Tecnología del Departamento de Comercio de los EE.UU. cuyos objetivos son elaborar y promover patrones de medición, normas y tecnología. Tiene una relación con la continuidad de negocios ya que, en su publicación 800-34 (Contingency Planning Guide for Information Technology Systems) de su serie 800 [NIST, 2010], desarrolla una guía de planes de contingencia de los sistemas de información de cualquier empresa.

British Standards Institution (BSI)

Es una institución independiente y global, la cual se basa en la creación de normas para lograr la estandarización de procesos, mejorar las prácticas de gestión y promover la innovación, proporciona soluciones basadas en estándares en más de 150 países. Es un organismo colaborador de ISO y proveedor de dichas normas.

BSI ayuda a las empresas, gobiernos y organizaciones de todo el mundo a aumentar la calidad y el rendimiento de una forma sostenible y socialmente responsable. BSI Group es reconocido a nivel mundial por la publicación de BS 25999 y la certificación como líder y proveedor de formación en este campo. En la actualidad, BSI apoya el despliegue de las nuevas Normas Internacionales de Continuidad de Negocio - ISO 22301 e ISO 22313.

Entre sus actividades principales se incluyen:

- Certificar sistemas de gestión y productos.
- Desarrollar normas nacionales e internacionales.
- Proporcionar formación e información sobre normas y comercio internacional.
- Realizar auditorías a las organizaciones.

2 MARCO TEORICO

2.1 Conceptos generales

DESASTRE

Tradicionalmente se ha entendido por desastre a un incendio o inundación, porque este tipo de eventualidades destruía recursos físicos de la organización como archivos, equipos o los registros vitales. En la actualidad, eliminados en gran medida estos riesgos, los altos directivos se enfrentan a una nueva forma de desastre, que afecta directamente a su activo principal, que es la información.

En cualquier momento, la informática de una empresa se puede quebrar total o parcialmente como consecuencia de un siniestro fortuito. Si, las operaciones más importantes de la empresa se suspenden repentinamente, será incalculable el daño causado al negocio y más aún a la reputación de esta. Entre las principales causas de desastres informáticos se tiene los siguientes.

- Fallo en el suministro y red eléctrica.
- Fallos en el hardware y los sistemas de almacenamiento.
- Fallos humanos.
- Fallos de software.
- Ataques maliciosos y virus informáticos
- Desastres naturales.

AMENAZA

Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización. NIST de los Estados Unidos de América 2008 lo define como: “Cualquier circunstancia o hecho que pueda afectar negativamente a las operaciones de la organización, sus activos de información o individuos a través del acceso no autorizado, destrucción, acceso, modificación de la información, y/o negación de servicio. Además, la posibilidad de una amenaza de fuente de explotar con éxito una vulnerabilidad de la información del sistema en particular. En otra acepción, son todas las actividades, eventos o circunstancias que pueden afectar el buen uso de un activo de información dañando el soporte a un proceso, perjudicando el logro de los objetivos de negocio”.

Figura 4. Tipos de Amenazas de Continuidad

Del Pino 2007

VULNERABILIDAD

Es la debilidad de un activo o grupo de activos que puede ser explotada y perjudicada por una o más amenazas. Son debilidades que pueden ser exploradas para convertir una amenaza en un riesgo real que pueden causar daños graves en una organización. Las vulnerabilidades son una o más condiciones que pueden permitir a una amenaza afectar a un activo. Según el BCI 2010: “Las vulnerabilidades en el negocio y en el modelo de operación de una organización pueden considerarse en siete áreas: reputación, cadena de suministro, información y comunicaciones, sedes e instalaciones, personas, finanzas y clientes”.

Se puede definir a la ausencia de controles o a su deficiente establecimiento como las principales causas de vulnerabilidad sobre los activos de una organización.

RIESGO

Potencial de que una amenaza – externa o interna – explote una vulnerabilidad de uno o varios activos ocasionando daño a la organización. Su naturaleza puede depender de aspectos operativos, financieros, regulatorios y administrativos (ISO 27005, 2008).

Según COSO en su “Marco de Gestión Integral de Riesgo” (2008): “Los riesgos son futuros eventos inciertos, los cuales pueden influir el cumplimiento de los objetivos estratégicos, operacionales, financieros y de cumplimiento”.

Causas de los Riesgos:

- Personal: Fallas cometidas por el personal. Ejemplo: Por falta de conocimiento.
- Procesos: Fallas causadas por debilidades en el diseño y/o ejecución de procesos de la organización como por ejemplo controles inadecuados.
- Sistemas: Fallas causadas por vulnerabilidades en los sistemas, como fallas de red o caídas de sistemas.
- Eventos externos: Fallas que resultan por cambios adversos en el entorno de la organización, por situaciones causadas por terceros o por desastres naturales.

Figura 5. Tipos de Riesgos

ISACA 2011

Identificar riesgos implica analizar causas de aparición, consecuencias, magnitud e impacto; así como definir criterios de aceptación y la implementación de controles.

IMPACTO

El Business Continuity Institute (2012) lo define como un “Evento que tiene la capacidad de provocar la pérdida de o la interrupción de las operaciones, servicios o funciones de la organización, el cual, si no se administra, puede escalar y convertirse en una emergencia,

crisis o desastre”. Su identificación y cuantificación es relevante en el proceso de la Gestión de Riesgos, que es el conjunto de actividades que permite analizar, tratar y evaluar los riesgos en las organizaciones.

Cabe mencionar que la valoración del impacto puede ser expresado de forma cuantitativa, es decir estimando las pérdidas económicas, o de forma cualitativa, asignando un valor dentro de una escala (alto, bajo, medio), también se recurre al análisis de grado de pérdida o daño que causaría una interrupción en un activo de información mediante el manejo de probabilidades de ocurrencia, ya que se utiliza para determinar si se invertirá en medidas para evitar dicha interrupción.

La interrupción se puede evitar teniendo un procedimiento que, o bien proporciona alguna forma alternativa de la continuidad del negocio o corrige el problema dentro de un tiempo aceptable. El impacto no siempre se produce inmediatamente después de una interrupción y la mayoría de las empresas pueden sobrevivir durante algún tiempo antes de que las pérdidas comiencen. Este período es vital para el negocio y varía entre empresas y líneas de negocio. Si se realiza un análisis de riesgos basado de tipo cuantitativo de impacto y las probabilidades, las escalas cualitativas del impacto son: catastrófico o extremo, grave, medio, moderado o bajo e insignificante probable.

A continuación se mostrará la matriz que se ajustará según las políticas que emplea la entidad referenciada en la presente tesis. Es decir, va a depender del tipo de organización y de los activos de información que se tengan para clasificar los riesgos y calcular los impactos.

		Nivel de riesgos o Nivel de Severidad				
Probabilidad	Casi Certeza	MODERADO	ALTO	ALTO	EXTREMO	EXTREMO
	Muy Probable	BAJO	MODERADO	ALTO	ALTO	EXTREMO
	Posible	BAJO	MODERADO	MODERADO	ALTO	ALTO
	Improbable	BAJO	BAJO	MODERADO	MODERADO	ALTO
	Rara	BAJO	BAJO	BAJO	BAJO	MODERADO
		Insignificante	Menor	Moderado	Mayor	Catastrófico
		Impacto				

Figura 6. Matriz de riesgos en un análisis cualitativo de impacto y probabilidad

BCI 2012

CONTROLES

Son las políticas, medidas de seguridad, procedimientos y prácticas para reducir riesgos y que proveen cierto grado de certeza de que se lograrán los objetivos del negocio. Estos permiten que se realicen las correcciones necesarias en caso se detecten eventos que escapan de su alcance.

Los objetivos relevantes de los controles son:

- Garantizar que mediante los mecanismos de control establecidos se logren las metas de la organización.
- Salvaguardar los activos de la organización para mantener la integridad de la información.

Preventivos	<ul style="list-style-type: none"> •Identifican problemas antes de que ocurran por medio de monitoreo constante. •Previenen errores, omisiones o actos maliciosos y reducen las vulnerabilidades. •Ejemplos: Contratar seguros para los activos, realizar copias de seguridad de los archivos.
Detectivos	<ul style="list-style-type: none"> •Identifican y reportan una amenaza, la ocurrencia de un error, omisión o acto malicioso en el momento en que estos ocurren. •Ejemplos: Auditorías internas, monitorización de eventos, revisiones periódicas de procesos.
Correctivos	<ul style="list-style-type: none"> •Minimizan el impacto de una amenaza y solucionan errores detectados por controles detectivos. •Modifican procedimientos para minimizar ocurrencias del problema. •Ejemplos: Planes de Contingencia y Restauración, parches de seguridad.
Disuasivos	<ul style="list-style-type: none"> •Reduce la probabilidad de ocurrencia de una amenaza •Ejemplos: Cámaras de Vigilancia.

Figura 7. Tipos de Controles

ISO 27001

2.2 Conceptos relacionados a la recuperación de desastres de TI

NORMAS TECNICAS

ISO 22301:2012

La norma ISO 22301:2012 Seguridad de la sociedad - Sistemas de gestión de la continuidad del negocio, es el nuevo estándar internacional para la gestión de continuidad del negocio. Se ha creado en respuesta al gran interés internacional en el original norma británica BS 25999-2 y otras normas regionales. Proporciona el mejor marco de referencia y es el nuevo estándar global para gestionar la continuidad del negocio en una organización.

Este estándar especifica requisitos para la creación y gestión de un negocio en efectivo de un SGCN. Es sólo para uso interno por y las partes externas, incluyendo organismos de certificación, para evaluar la capacidad de organización para cumplir los requisitos reglamentarios y del cliente así como los propios de la organización. La ISO 22301 contiene sólo aquellos requisitos que pueden ser auditados objetivamente, por lo tanto puede ser utilizado por una organización para asegurar que las partes interesadas usen un SGCN apropiadas en su lugar; y ha sido diseñada para lograr una mayor seguridad social (proporcionar protección de la sociedad, y responder a, incidentes, emergencias y desastres provocados por actos humanos intencionales, riesgos naturales y fallas técnicas).

La ISO 22301 ha remplazado a la norma británica BS 25999-2. Estas dos normas son bastante similares, pero la ISO 22301 puede ser considerada como una actualización de la BS 25999-2 y a diferencia de la norma británica ha sido aceptada por institutos de normas nacionales en 163 países.

Según John Sharp “Las adiciones en la ISO/IEC 22301 han añadido más profundidad y claridad, mientras que las omisiones no son detrimento de las prácticas de BCM, en general son buenos principios”. Lo cierto es, que esta nueva norma pone mucho más énfasis en la comprensión de requisitos, el establecimiento de los objetivos y en la medición del desempeño y se mantienen los aspectos más importantes de la continuidad de negocio como son el análisis del impacto, la estrategia y la planificación.

Al igual que la norma predecesora, ISO 22301 es una norma adecuada para todo tipo de organización, grande o pequeña y perteneciente a cualquier sector. Es especialmente empleada para organizaciones que operan en sectores críticos de riesgo, como finanzas, transporte, telecomunicaciones y sector público, donde la necesidad de continuar la actividad comercial es primordial para el beneficio de la organización, los clientes y los interesados.

ISO 27031:2011

La norma ISO 27031:2011 Tecnología de Información - Técnicas de Seguridad - Directrices para la preparación de la información y tecnología de comunicación para la continuidad del negocio, es un estándar que ayuda a las organizaciones a prepararse para los incidentes, responder a riesgos de seguridad y ser menos susceptible a interrupciones.

Describe los conceptos y principios de la preparación de las tecnologías de la información y las comunicaciones (TIC) para la continuidad del negocio, y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos (tales como los criterios de desempeño, diseño e implantación) para la mejora de la preparación de las TIC de una organización para garantizar la continuidad del negocio. Se aplica a cualquier organización (privadas, gubernamentales y no gubernamentales, independientemente de su tamaño) desarrollando su programa de adecuación de las TIC para la continuidad del negocio, y exigiendo que sus servicios e infraestructura TIC estén listos para apoyar las operaciones de negocios en el caso de nuevos eventos e incidentes, y las interrupciones relacionadas que puedan afectar la continuidad (incluida la seguridad de la información) de las funciones críticas del negocio. También permite a una organización medir los parámetros de

desempeño correlacionados con su Continuidad de Negocio de una manera consistente y reconocida.

El ámbito de aplicación de esta norma abarca todos los eventos e incidentes (incluidos los relacionados con la seguridad de la información) que podrían tener un impacto en la infraestructura de las TIC y en los sistemas. Incluye y extiende las prácticas de manejo y gestión de incidentes de seguridad de la información y la planificación de la preparación de las TIC y sus servicios).

La norma incorpora el enfoque cíclico PDCA de la norma ISO 9000, extendiendo la continuidad convencional de procesos de negocio que plantean tener más en cuenta las TIC. Incorpora “fracaso métodos de evaluación correspondientes a los escenarios como FMEA (Análisis de Modo de Falla y Efectos), con énfasis en la identificación de sucesos desencadenantes que podrían precipitar incidentes graves”.

ISO 27001 / 27002

Es la norma internacionalmente reconocida para la Gestión de Seguridad de la Información (ISO 27001) y su Código de Práctica (ISO 27002), ambas contemplan la continuidad de negocio como un elemento clave dentro de la gestión de la seguridad de la información.

Tiene como fin, contrarrestar interrupciones en las actividades empresariales y en los procesos críticos de negocio derivados de fallos importantes en los sistemas de información y garantizar su reanudación. Esta norma indica que crear un SGSI es vital para preservar la Continuidad del Negocio. En la siguiente tabla se muestra la relación entre La gestión de Riesgos de la ISO 27001 y la Gestión de Continuidad de Negocio de la ISO 22301.

ELEMENTO	ISO 27001: Gestión de Riesgos	ISO 22301: Gestión de Continuidad de Negocio
Herramienta Método	Análisis de Riesgos (AR)	Análisis de Impacto del Negocio (BIA)
Claves	Impacto y Probabilidad	Impacto y Tiempo
Tipos de Incidente	Todo tipo de eventualidades (segmentadas)	Fallos críticos para el negocio (no segmentadas)
Magnitud	Toda, generalmente segmentada	Incidentes estratégicos críticos para el negocio.
Enfoque	PREVENTIVO: Gestión de Riesgos para los objetivos del negocio.	CORRECTIVO: Gestión de Incidentes
Escenarios e Intensidad	Todos (segmentados)/Toda	El peor escenario(s)/Incidentes súbitos

Figura 8. Matriz de relación entre la ISO 27001 y la ISO 22301

BSI 2012

Además en el capítulo 14 de la ISO/IEC27002 se tratan los siguientes aspectos de la seguridad de información y de la gestión de la continuidad del negocio:

- Incluir la seguridad de la información y evaluación de riesgos en el proceso de gestión de continuidad del negocio.
- Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la Información.
- Marco referencial de la planeación de la continuidad del negocio.
- Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio.

COBIT

Objetivo de Control para la Información y la Tecnología relacionada, conocido como COBIT, es una herramienta para la administración de las tecnologías de información. Desarrollada por ISACA como un estándar para la seguridad de la tecnología de información y buenas prácticas de control. Constituye un marco unificador internacionalmente aceptado como una buena práctica para la gestión, el control de la información, de la tecnología de información y de los riesgos que estas sufren. “Esta última versión incorpora la última evolución de pensar en la gobernabilidad empresarial y técnicas de gestión, y establece los principios globalmente aceptados, prácticas, herramientas y modelos analíticos para ayudar a aumentar la confianza en, y el valor de los sistemas de información. Además incorpora la

integración de otros marcos importantes, normas y recursos, incluyendo Val IT , Risk IT , BMIS (Business Model for Information Security), ITAF (IT Assurance Framework)”.

Las organizaciones pueden beneficiarse en la utilización de este marco para el manejo de continuidad de negocio, el cual les permitirá tener enfoques coherentes y mensurables ante interrupciones no planificada de servicios de TI.

Figura 9.Principios de COBIT

ISACA 2012

NFPA 1600:2010

El NFPA 1600 establece una base de normalización para el planeamiento y operaciones de manejo de desastres/ emergencias al brindar elementos comunes del programa, técnicas, y procedimientos enfocados en su totalidad en el programa. Esta norma establece los componentes importantes de un plan que permita a las organizaciones desarrollar un programa para satisfacer sus necesidades particulares.

Algunos de los elementos más importantes mencionados son:

- Identificación de peligros, evaluación de riesgos y su mitigación: La evaluación de riesgos debe cuantificar la probabilidad de incidentes y la gravedad de sus consecuencias. Se debe cuantificar el impacto que tendría un desastre en sus activos, así como las consecuencias financieras directas o indirectas. El análisis del impacto debe cuantificar las emergencias potenciales de un riesgo, que permita evaluar el

costo-beneficio por los esfuerzos de investigación y determinar cuánto invertir en planes de mitigación, respuesta y recuperación.

- Administración de recursos: Los recursos necesarios deben ser catalogados para su recuperación, y el acceso a éstos debe disponerse con anterioridad. Cualquier limitación debe ser identificada para que fallas puedan ser corregidas.
- Planificación: Todas las organizaciones deben tener un plan que cumpla con el reglamento, este debe contar con estrategias de mitigación a corto y largo plazo, una lista de funciones críticas, en orden de prioridades, un análisis de impacto, un programa de respuesta y recuperación total y un plan de evacuación.
- Dirección, control y coordinación: Toda organización debe contar con un sistema de administración de incidentes (IMS) y procedimientos para el control constante de incidentes.

El NFPA 1600 es una norma que establece un conjunto común de criterios para mitigar, prepararse, responder y recuperarse ante desastres y emergencias, ha sido aprobada por el Instituto Americano Nacional de Normas y respaldado por la Asociación de Manejo de Emergencias y la Asociación internacional de Gerentes.

NIST SP 800-34

Proporciona conocimientos, recomendaciones y consideraciones para los planes de contingencia. Los planes de contingencia están diseñados para mitigar el riesgo de una variedad de interrupciones que van desde leves a graves, mediante la gestión de soluciones eficaces y eficientes para el mejoramiento de la disponibilidad del sistema. Así mismo, no es posible eliminar todos los riesgos por completo.

El objetivo de la resiliencia en las organizaciones es permitir el continuo funcionamiento de sus actividades durante cualquier tipo de interrupción.

EL ISCP se diferencia del DRP debido a que se puede ejecutar desde la ubicación actual del sistema así como desde la ubicación alterna. Una vez que el DRP es activado con éxito en el sitio alternativo cada sistema afectado utiliza su respectivo ISCP para la restauración, recuperación y pruebas para poner este en operación.

El Plan de Emergencia del Ocupante describe el procedimiento para los ocupantes de una instalación en caso de amenaza o incidente de salud, seguridad del personal, del medio ambiente o de la propiedad.

CONCEPTOS DIRECTAMENTE RELACIONADOS

BIA (Business Impact Analyst)

BIA es el proceso que consiste en analizar las funciones del negocio y el efecto que una interrupción del negocio pudiera causar sobre ellas. De acuerdo al BCI es “el análisis a nivel de gestión por el cual una organización evalúa los impactos cuantitativos y cualitativos, los efectos y la pérdida que podría resultar si se tuviera que sufrir una emergencia, incidente o crisis. Los hallazgos de un BIA se utiliza para tomar decisiones sobre la estrategia de Continuidad del Negocio y soluciones”.

Un BIA ayuda a identificar lo que se perderá si el negocio se interrumpe, lo que podría costar la pérdida de beneficios e ingresos, el deterioro de las relaciones con los clientes, pérdida de reputación. También es un proceso clave para entender cuánto de una interrupción cada proceso o tarea puede tolerar antes de que el daño sea irremediable y de cuales recursos (personas, máquinas, documentos u otros procesos) depende la empresa.

Los propósitos de un BIA para cada actividad, producto o servicio son:

- Documentar los impactos en tiempo que se derivarán de su pérdida o interrupción.
- Identificar el Máximo Periodo Tolerable de Interrupción (MTPD).
- Identificar las dependencias—tanto internas como externas— que son necesarias para que la actividad funcione de forma eficaz.

BIA es la base para la toma de decisiones y la planificación estratégica de recuperación en la cual la estructura de gestión de la continuidad reside y es sin duda uno de los resultados más importantes y fundamentales del ciclo de vida de la continuidad del negocio. Es a través del BIA que las necesidades de la organización en respuesta a un desastre pueden ser adecuadamente evaluadas y priorizadas.

Business Continuity Plan (BCP)

El plan de continuidad de negocios es un conjunto de procedimientos documentados e información que ha sido desarrollada, recopilada y mantenida a disposición para su uso durante un incidente, para permitir a la organización continua con la entrega de sus actividades más importantes y urgentes a un nivel aceptable predefinido. El plan de continuidad de negocios se actualiza y mantiene a través del proceso de BCM que se definió anteriormente. Este reducirá el número y la magnitud de las decisiones que se toman durante

un período en que los errores pueden resultar mayores. El Plan establecerá, organizará y documentará los riesgos, responsabilidades, políticas y procedimientos, acuerdos con entidades internas y externas.

Un claro ejemplo de la ausencia de un plan de continuidad de negocios es cuando se malogra el disco duro de una computadora, en realidad no cuesta nada repararlo, pero el daño y el impacto que puede causar es inmensurable si es que no hay ningún plan de mitigación ante su pérdida (mitigación podría ser alguna forma de copia de seguridad, por ejemplo).

Como menciona Hotchkiss [2010, p. 26.]. “Eventos de pequeño impacto también pueden causar daño en términos de tiempo de reparación”, como en el ejemplo antes mencionado, una pequeña deficiencia puede causar un impacto bastante limitado en negocio, pero puede llegar a costar un montón de dinero para reparar debido a la falta de planificación. Esto significa que se debe tener en cuenta el impacto y el daño, así como el costo de recuperación llegar a una idea razonable del costo de no tener un plan de continuidad.

Los elementos claves de un BCP son:

- Respuesta a la emergencia: Respuesta inmediata a una emergencia. Por ejemplo un Plan de Evacuación.
- Gestión del Incidente: La gestión de Respuesta al incidente como por ejemplo un Plan de Continuidad en Crisis.
- Continuidad: La repuesta inicial del negocio para asegurar que las actividades esenciales pueden continuar operando a un nivel mínimo aceptable.
- Recuperación: Un plan para recuperar actividades a un nivel sostenible.
- Reanudación: Un plan para reanudar las operaciones de la organización.

Un Plan de Continuidad de Negocio (BCP) está formado por los siguientes planes:

Plan de Emergencia, Plan de Comunicación de Crisis, Plan de Gestión de Crisis y Plan de Recuperación de Desastres.

Disaster Recovery Plan (DRP)

Es un proceso documentado o conjunto de procedimientos o acciones para recuperar y proteger la infraestructura de TI de una organización en caso de un desastre. Refiriéndose con desastre a todo evento súbito, imprevisto catastrófico que interrumpe los procesos de negocio lo suficiente como para poner en peligro la viabilidad de la organización .Un

desastre podría ser el resultado de un daño importante a una parte de las operaciones, la pérdida total de una instalación, o la incapacidad de los empleados para acceder a esa instalación. El DRP es una declaración exhaustiva de acciones coherentes que deben tomarse antes, durante y después de un desastre".

El Plan de Recuperación de Desastres tiene como objetivo proporcionar un marco para la reconstrucción de las operaciones vitales de la organización, para garantizar la seguridad de los empleados y la reanudación de las operaciones sensibles a tiempo y los servicios en caso de una emergencia.

El DRP incluye la planeación de pasos para evitar riesgos y mitigarlos, DRP es aplicable en todos los aspectos de un negocio, sin embargo se utiliza normalmente en el contexto de operaciones para el procesamiento de datos.

Beneficios de un Plan de Recuperación ante un desastre:

- Permite a la organización evitar riesgos de retrasos o mitigar el impacto de estos al: minimizar potenciales pérdidas económicas y; decrementar la exposición a escenarios de desastre.
- Reducir la probabilidad de que ocurran al mejorar la capacidad de recuperar las operaciones normales del negocio.
- Reducir las interrupciones de la operación.
- Provee un procedimiento pre- planificado minimizando el tiempo de toma de decisiones en caso de desastre.
- Elimina la confusión y reduce la probabilidad de error humano debido al estrés que produce una crisis.
- Protege los activos de la organización incluyendo al recurso humano.

Los planes de recuperación de desastres TI facilitan procedimientos detallados a seguir, paso a paso, para recuperar los sistemas y redes que han tenido interrupciones y ayudar a simplificar la normalidad en las operaciones. El objetivo de estos procesos es reducir cualquier impacto negativo en las operaciones de la organización. El proceso de recuperación de desastres identifica los sistemas y redes críticos de TI; fija las prioridades para su recuperación y dibuja los pasos necesarios para reiniciar, reconfigurar y recuperar dichos sistemas y redes. Todo plan integral de recuperación de desastres debe incluir a todos los proveedores más relevantes, las fuentes de experiencia para recuperar los sistemas

afectados y una secuencia lógica de los pasos a seguir hasta alcanzar una recuperación óptima.

Teniendo en cuenta que se ha realizado una evaluación de riesgos e identificado amenazas a nuestra infraestructura y plataforma de TI, el siguiente paso será determinar qué elementos de dicha infraestructura y plataforma son los más importantes para las operaciones organizacionales. Además, asumiendo que los sistemas y redes TI funcionan con normalidad, la organización deberá ser plenamente viable, competitiva y sólida desde el punto de vista financiero. Cuando un incidente afecta de manera negativa a la infraestructura y plataforma de TI, las operaciones corporativas pueden verse amenazadas.

Los pasos que se deben seguir para la elaboración del DRP será la elaboración de la declaración de políticas para el DRP TI, contar con unas directivas formales proporcionan la autoridad y orientación necesaria para elaborar un DRP TI efectivo. Realización del análisis de impacto sobre el negocio (BIA). El análisis del impacto sobre el negocio ayuda a identificar y priorizar los sistemas y componentes críticos de TI. Identificación de controles preventivos, medidas que reducen los efectos de las interrupciones al sistema y pueden aumentar su disponibilidad y reducir los costos. Desarrollo de estrategias de recuperación, tener una estrategia integral garantiza que el sistema se recuperará de manera rápida y efectiva después de una interrupción. Desarrollo del DRP TI, el Pla de Recuperación de Desastres debe contener orientaciones y procedimientos detallados para la restauración del sistema dañado. Prueba, formación y ejecución del plan, la prueba del plan identifica vacíos en la planificación, mientras que la formación prepara al personal de recuperación para la activación del plan; ambas actividades mejoran la eficacia del plan y la preparación general de la entidad. Mantenimiento del plan, el plan debería ser un documento vivo que se actualiza regularmente para mantenerlo al día con mejoras al sistema.

La ampliación de cada paso del Plan de Recuperación de Desastres de TI son los siguientes.

- El equipo de implementación del plan debería reunirse con el equipo interno de TI, el equipo de aplicación y los administradores de redes, y establecer el alcance de la acción, como por ejemplo, elementos internos, activos externos, recursos de terceros y enlaces a oficinas/clientes/proveedores; debemos asegurarnos de informar a la dirección del departamento de TI sobre dichas reuniones para que estén bien informados.

- Recopilar todos los documentos relevantes de la infraestructura de redes, como los diagramas de las redes, la configuración de los equipos y bases de datos.
- Obtener copias de los planes de recuperación de redes y de TI existentes; si no los hay, proceder con los siguientes pasos.
- Identificar las amenazas contra la infraestructura de TI que la dirección considere más preocupantes: por ejemplo, incendios, errores humanos, apagones de energía, fallo de los sistemas.
- Identificar aquello que la dirección considera que son las principales vulnerabilidades de la infraestructura: por ejemplo, inexistencia de sistemas de respaldo en caso de apagón eléctrico, copias de bases de datos obsoletas.
- Examinar el historial previo de apagones y interrupciones, y cómo fueron gestionados por la empresa.
- Identificar los activos TI que la dirección considera de importancia crítica. Por ejemplo: centro de llamadas, granjas de servidores, acceso a internet.
- Determinar el tiempo máximo de apagón eléctrico que está dispuesta a aceptar la dirección en caso de indisponibilidad de los equipos TI.
- Identificar los procedimientos operativos que se utilizan actualmente para responder a los apagones críticos.
- Determinar cuándo se probaron estos procedimientos para validar si siguen siendo adecuados o no.
- Identificar el/los equipo/s de respuesta de emergencia para todas las interrupciones de la infraestructura crítica de TI; determinar su nivel de conocimientos y preparación para manejar los sistemas críticos, especialmente en casos de emergencia.
- Identificar las capacidades de respuesta de los proveedores en casos de emergencia; si se han utilizado alguna vez; si funcionaron correctamente; cuánto paga la compañía por estos servicios; el estado del contrato de servicio; la existencia del acuerdo de nivel de servicio (SLA) y si se usa alguna vez.
- Recopilar los resultados de todas las evaluaciones en un reporte de análisis de carencias que identifique lo que se está haciendo frente a lo que debería hacerse, con recomendaciones sobre cómo lograr el nivel requerido de preparación y las inversiones necesarias para ello.
- Lograr que la dirección lea el reporte y acuerde tomar las acciones recomendadas.

- Preparar un plan de recuperación de desastres IT que cubra los sistemas y las redes esenciales de TI.
- Realizar pruebas de los planes y activos de recuperación de sistemas para validar su operatividad.
- Actualizar la documentación del plan de RD para que recoja los cambios efectuados.
- Programar la próxima revisión/auditoría de capacidades de recuperación de desastres TI.

Alguno de los aspectos importantes que se deberá tener en cuenta antes de iniciar con una planificación de un DRP de TI son los siguientes:

Apoyo de la alta gerencia. Asegúrese de tener el apoyo de la alta gerencia a fin de lograr alcanzar los objetivos del plan.

Tomarse en serio el proceso de planificación de DRP de TI. Aunque la recopilación y análisis de los datos para el DRP de TI puede llevar mucho tiempo, no es necesario que tenga docenas de páginas. Los planes simplemente necesitan la información correcta, y esa información debería ser actual y precisa. Es esencial reunir y organizar la información correcta. Estudiar los resultados con las unidades de negocio. Una vez finalizado el plan de recuperación de desastres, debemos cotejar sus conclusiones con los líderes de las unidades de negocio para comprobar que nuestras premisas son correctas.

Flexibilidad. La plantilla sugerida en este artículo puede ser modificada en lo que sea necesario para conseguir nuestros objetivos

2.3 Marco regulatorio legal

NTP 27001: 2013

Norma Técnica Peruana de Seguridad de Información es una norma elaborada por el Comité Técnico de Normalización de codificación e Intercambio Electrónico de Datos (EDI) en el año 2008, utilizando como antecedente las ISO/IEC 27001:2013.

Tiene como objetivos proporcionar un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de Seguridad de Información como una buena práctica de la gestión de la seguridad.

Cabe mencionar que se hará mayor énfasis en lo relacionado de esta norma a la continuidad de negocios. Comprende de 11 ítems de control de seguridad que envuelven un total de 39

categorías principales, los cuales se muestran a continuación, enfatizando en el ítem de continuidad:

- Política de seguridad
- Seguridad Organizacional
- Gestión de Activos
- Seguridad en Recursos Humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de incidentes en la Seguridad de Información
- Gestión de continuidad del negocio

Aspectos de la gestión de continuidad del negocio: Reaccionar ante las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los activos y asegurar la reanudación oportuna.

Este ítem en particular menciona que las formas de lograr una buena continuidad de negocio son:

- Incluyendo la seguridad de información en la gestión de la continuidad del negocio, para ello se deben establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta efectiva ante cualquier tipo de incidente.
- Relacionando la continuidad de negocios con la evaluación de riesgos, para ello deben ser identificadas las amenazas que pueden causar interrupciones, así como las probabilidades e impacto de dichas interrupciones.
- Desarrollando e implementando planes de continuidad que incluyan la seguridad de información.
- Contando con un marco de planificación de la continuidad del negocio, con el fin de asegurar consistencia e identificar prioridades de prueba y mantenimiento.
- Probando, manteniendo y reevaluando los planes de continuidad del negocio, con el fin de asegurar que estén actualizados y sean efectivos.
- Cumplimiento.
-

SARBANES OXLEY (SOX)

La entidad educativa superior al pertenecer a una red global de educación universitaria de excelencia, tiene que cumplir con las regulaciones de la legislación de Sarbanes Oxley (SOX).

Creada en el 2002 de la voluntad de controlar las empresas que cotizan en la bolsa de Nueva York y sus filiales, para evitar que los procesos con transacciones económicas pudieran ser alterados de forma fraudulenta. Establece requerimientos de seguridad relacionados con la continuidad del negocio (los artículos 302, 404 y 409 afectan a la continuidad de negocio). Hace varios años que SOX traspasó las fronteras y actualmente existen versiones de la misma en Japón (llamada JSOX) o en la Unión Europea (llamada Euro SOX).

2.4 Metodologías

Gestión de riesgos - MAGERIT

El Análisis de Riesgos va a permitir identificar claramente las amenazas a las que se encuentran expuestos los diferentes activos de información, pudiendo estimar la frecuencia de materialización de tales amenazas y valorar el impacto al materializarse dicha amenaza.

Teniendo en cuenta que la ISO 27005 no proporciona una metodología en sí de Análisis de Riesgos, sino más bien describe en sus cláusulas todo el proceso recomendado de análisis en donde se incluyen las fases que lo conforman, se hace imprescindible mencionar a MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las administraciones públicas) en su versión 3, que es una metodología de análisis y gestión de riesgos, elaborada por el Consejo superior de Administración Electrónica CSAE de España, la cual facilita la gestión de los riesgos, esta metodología fue concebida en función del creciente uso de las tecnologías por parte de la sociedad y las organizaciones que permiten conseguir el cumplimiento de sus objetivos, sin embargo asociadas a ese beneficio se incorporan ciertos riesgos que deben minimizarse, y poder establecer una adecuada gestión de los riesgos es de suma importancia.

La metodología está incorporada en 3 partes que son:

- Método: Describe la estructura que debe tener el modelo de gestión de riesgos acorde a lo que propone ISO para la gestión de riesgos, contiene consejos y aspectos prácticos lo cual facilita esta tarea.

- Catálogo de Elementos: Prácticamente es una especie de inventario, en donde se establecen los activos de información y características que deben tomarse en cuenta al momento de valorarlos, junto con un listado de amenazas y controles, además nos indica cómo desarrollar un informe.
- Guía de Técnicas: Describe técnicas utilizadas en el análisis de riesgos y ejemplos con tablas, algoritmos, árboles de ataque, análisis de costo beneficio, diagramas de flujo y buenas prácticas.

La metodología de MAGERIT cabe perfectamente dentro de la Implementación de la gestión de riesgos expresada en la Norma ISO 31000, a lo que se denomina “Proceso de Gestión de los Riesgos”.

*Figura 10.*Marco de trabajo para la gestión de riesgos

ISO 31000, 2012

Con una visión en conjunto MAGERIT afronta 2 tareas importantes que permiten definir claramente un proceso de Gestión de Riesgos, siendo el Análisis y el Tratamiento del riesgo.

*Figura 11.*Gestión de Riesgos

MAGERIT v3, Libro I Método

Donde el Análisis establece los siguientes elementos:

Activos: Todos los elementos que forman parte del Sistema de Información y que soportan la misión de la Organización.

Amenazas: Todo incidente no deseado sobre el activo, que provoca un daño y perjuicio a la Organización.

Salvaguardas: Implementación de medidas que eviten que las amenazas no causen mucho daño. En base a estos elementos se pueden estimar, el impacto de lo que se podría producir.

El riesgo, probabilidad de que ocurra

Figura 12. Proceso de gestión de riesgos

MAGERIT v3, Libro I Método

ANÁLISIS DE IMPACTO DE NEGOCIO – BIA

El proceso para determinar el Análisis de Impacto de Negocio son los siguientes.

- Determinar los procesos de negocio y criticidad de recuperación. El sistema admite el soporte y el impacto de una interrupción del sistema, en estos procesos se determina el impacto de la interrupción y el tiempo de inactividad estimado. El tiempo de inactividad debe reflejar el tiempo máximo que una organización puede tolerar mientras mantiene el proceso.
- Identificar los requerimientos de recursos. Los esfuerzos de recuperación reales requieren una evaluación completa de los recursos necesarios para reanudar los

procesos de negocio y las interdependencias relacionadas lo más rápido posible. Ejemplos de recursos que deben identificarse incluyen instalaciones, personal, equipos, software, archivos de datos, componentes del sistema y registros vitales.

- Identificar las prioridades de recuperación para los recursos del sistema. Basado en los resultados de las anteriores actividades, los recursos del sistema se pueden vincular más claramente a los procesos críticos de negocios y sus funciones. Se pueden establecer niveles de prioridad para secuenciar actividades y recursos de recuperación.

El proceso BIA muestra las actividades de recopilación de datos, que se describen en esta sección, consiste en un sistema de información representativo con múltiples componentes (servidores), están diseñados para ayudar al coordinador de ISCP a racionalizar y enfocar las actividades de desarrollo del plan de contingencia para lograr un Plan más efectivo.

Figura 13. Proceso BIA

NIST SP 800-34

Un sistema de información puede ser muy complejo y, a menudo, admite múltiples procesos de negocio, resultando en diferentes perspectivas sobre la importancia de los servicios o capacidades del sistema. Para lograr el BIA y comprender mejor los impactos que una interrupción o interrupción del sistema puede tener en la organización, el Coordinador ISCP debe trabajar con la gerencia y puntos de contacto (POC) internos y externos para identificar y validar los procesos de negocio y los procesos que dependen de la información que se respalda del sistema. Los impactos de los procesos identificados son luego analizados en términos de disponibilidad, integridad, confidencialidad, y el nivel de impacto establecido para el sistema de información.

Se requiere que las organizaciones categoricen sus sistemas de información como de bajo impacto, impacto moderado o alto impacto para los objetivos de seguridad de confidencialidad, integridad y disponibilidad. El objetivo de seguridad de disponibilidad sirve como base del BIA. La identificación adicional de los procesos e impactos adicionales del negocio capta único propósito del sistema. La singularidad de la organización y el sistema son consideraciones importantes para la planificación de contingencias y el impacto comercial. Agregar tipos de información para abordar esta singularidad mejorará la priorización de los impactos de los componentes del sistema. Los procesos e impactos únicos se pueden expresar en valores o unidades de medida que sean significativos para la organización. Los valores se pueden identificar mediante una escala y se deben caracterizar como una indicación de la gravedad del impacto para la organización si el proceso no se pudiera llevar a cabo. Por ejemplo, se puede crear una categoría de impacto como "Costos" con valores de impacto expresados en términos de dotación de personal, tiempo de trabajo o costos relacionados con honorarios.

El Coordinador de ISCP (Information System Contingency Planning) debe analizar los procesos de negocio soportados y, junto con los propietarios del proceso, los líderes de liderazgo y de negocios, determinar el tiempo de inactividad aceptable si un proceso determinado o datos específicos del sistema se interrumpieron o no estaban disponibles. El tiempo de inactividad se puede identificar de varias maneras.

Tiempo máximo de inactividad tolerable (MTD). El MTD representa la cantidad total de tiempo que el propietario del sistema está dispuesto a aceptar para una interrupción o interrupción del proceso de negocio e incluye todas las consideraciones de impacto. La determinación de la MTD es importante porque podría dejar a los planificadores de contingencias con una dirección imprecisa en la selección de un método de recuperación apropiado y la profundidad de los detalles que se requerirán al desarrollar procedimientos de recuperación, incluidos su alcance y contenido.

Objetivo de tiempo de recuperación (RTO). RTO define la cantidad máxima de tiempo que un recurso del sistema puede no estar disponible antes de que haya un impacto inaceptable en otros recursos del sistema, procesos de negocios compatibles y el MTD. Determinar el recurso del sistema de información RTO es importante para seleccionar las tecnologías apropiadas que sean más adecuadas para cumplir con el MTD. Cuando no es factible cumplir

inmediatamente con el RTO y el MTD es inflexible, se debe iniciar un Plan de acción y un hito para documentar la situación y plan para su mitigación.

Objetivo de punto de recuperación (RPO). El RPO representa el punto en el tiempo, antes de una interrupción o interrupción del sistema, en el que se pueden recuperar los datos del proceso de negocio (dada la copia de seguridad más reciente de los datos) después de una interrupción. A diferencia de RTO, RPO no se considera como parte de MTD. Más bien, es un factor de cuánta pérdida de datos puede tolerar el proceso de negocio durante el proceso de recuperación.

Debido a que el RTO debe garantizar que el MTD no se exceda, el RTO normalmente debe ser más corto que el MTD. Por ejemplo, una interrupción del sistema puede impedir que se complete un proceso en particular, y debido a que lleva tiempo reprocesar los datos, ese tiempo de procesamiento adicional debe agregarse al RTO para permanecer dentro del límite de tiempo establecido por el MTD.

El Coordinador de ISCP, trabajando con la administración, debe determinar el punto óptimo para recuperar el sistema de información al abordar los factores mencionados anteriormente, al tiempo que equilibra el costo de la inoperatividad del sistema con el costo de los recursos necesarios para restaurar el sistema y su apoyo general para los procesos críticos de negocio.

Figura 14. Balance de costo

NIST SP 800-34

Los esfuerzos de recuperación real requieren una evaluación exhaustiva de los recursos necesarios para reanudar los procesos de negocios lo más rápido posible. Al trabajar con la administración y los POC (Point Of Contact) internos y externos asociados con el sistema, el Coordinador de ISCP debe asegurarse de que se identifiquen los recursos completos del sistema de información. Se puede usar una tabla simple para capturar los recursos relevantes del sistema de información.

Tabla 1
Sistema de información de recursos, tabla de componentes

System Resource/Component	Platform/OS/Version (as applicable)	Description
<i>Application Server</i>	<i>Sun V245/ Solaris / v10.0</i>	<i>Serves as the main application server</i>

Nota: NIST SP 800-34

Desarrollar prioridades de recuperación es el último paso del proceso BIA. Las prioridades de recuperación pueden establecerse de manera efectiva teniendo en cuenta la criticidad del proceso de negocio, los impactos de interrupción, el tiempo de inactividad tolerable y los recursos del sistema. El resultado es una jerarquía de prioridad de recuperación del sistema de información. El Coordinador de ISCP debe considerar las medidas y tecnologías de recuperación del sistema para cumplir con las prioridades de recuperación.

3 DEFINICION DEL PROBLEMA

3.1 Alcance de DRP

Al contar la institución educativa con la identificación de sus funciones y recursos críticos, es posible cumplir con su misión en caso de presentarse una contingencia que afecte su Sala de Servidores ubicado en la ciudad de Lima en el distrito de Santiago de Surco, y conocer cómo va a impactar financieramente estas interrupciones a sus funciones o procesos críticos. El plan proporcionará una descripción de las responsabilidades individuales y los procedimientos necesarios para restaurar los servidores y las telecomunicaciones en el menor tiempo posible. También permitirá que el centro alternativo proporcione la comunicación continua, identificada por institución para cumplir su misión.

En muchos casos, la importancia de contar con un DRP eficaz, consistente y actualizado que permita minimizar el tiempo de interrupción de los servicios informáticos en una compañía, se hace evidente cuando se producen situaciones de desastres que ponen en riesgo los activos informáticos, generando consecuencias desfavorables para la organización.

Por ello, antes de que ocurra un desastre informático, es fundamental que la empresa evalúe el costo económico de perder sus datos, poner en riesgo su imagen, perder clientes actuales y futuros y, por supuesto, las implicancias de detener las operaciones propias de la compañía, para así darse cuenta de lo indispensable que resulta contar con un sistema DRP.

3.2 Análisis de riesgos de continuidad de DRP

Se realizó el análisis de riesgos correspondiente a la organización, de los cuales, se identificaron seis escenarios de riesgos, se expresa la posibilidad de ocurrencia, se listan las causas de cada escenario, así como el efecto que causaría en la institución.

Tabla 2
Escenarios de riesgos

Cód.	Escenario	Riesgo (Existe la posibilidad de)	Causas (Dado que)	Efectos
R1	Indisponibilidad de acceso al centro de cómputo principal.	No se puede ingresar a la sede principal, donde se encuentra el centro de cómputo, y que todos los activos se encuentren intactos (sin ningún daño físico).	<ol style="list-style-type: none"> 1. Ocurra una huelga en contra de UPC por personas externas. 2. Ocurra una huelga por parte de trabajadores de UPC. 3. Accidente de tránsito con heridos graves y/o fallecidos. 4. Amenazas de Bomba, materiales peligrosos (gas tóxico, etc.). 5. Protestas de alumnos en contra de UPC. 	Interrupción en la operación de los procesos críticos que son soportados por los sistemas de información
R2	Pérdida total del data center principal.	No se puede ingresar a la sede principal, donde se encuentra el centro de cómputo, y todos los activos se encuentran destruidos.	<ol style="list-style-type: none"> 1. Incendio no controlado 2. Inundación de sitio principal. 	Interrupción en la operación de los procesos críticos que son soportados por los sistemas de información
R3	Indisponibilidad de la Información.	No se cuente con la información o los sistemas por algún problema tecnológico	<ol style="list-style-type: none"> 1. Falla de los Aplicativos o Sistemas Críticos. 2. Falta de Energía en el Centro de Cómputo. 3. Falla de seguridad lógica. 4. Lentitud en los sistemas críticos. 5. Ataque Cibernético DoS. 	Interrupción en la operación de los procesos críticos que son soportados por los sistemas de información
R4	Indisponibilidad de especialistas de TI (Recurso Humano).	No se cuente con el personal suficiente para realizar los subprocesos críticos de UPC.	<ol style="list-style-type: none"> 1. Epidemias o Pandemias: Puede dar lugar a bajas del personal clave por periodos prolongados de tiempo. 2. Pérdida o fallecimiento de personal clave (por accidente, intoxicación, enfermedades graves, etc.) 3. Rotación de personal. 	Interrupción en la operación de los procesos críticos que son soportados por los sistemas de información
R5	Indisponibilidad de	No se cuente con los servicios brindados	<ol style="list-style-type: none"> 1. Interrupción del servicio por problemas externos a la institución. 2. Falta o falla de proveedor de Internet o fluido eléctrico. 	Interrupción en la operación de los procesos críticos que

	Proveedores Críticos.	por el proveedor de sistemas u otros.		son soportados por los sistemas de información
R6	Evento sísmico, terremoto grado 8 con epicentro en Lima.	Ocurra un terremoto en Lima y Callao.	1. Desastres naturales (Terremotos, Tsunamis, etc.) que afecta personas, tecnología, instalaciones y proveedores.	Interrupción en la operación de los procesos críticos que son soportados por los sistemas de información

Luego de haber identificado los posibles escenarios de amenazas, procedemos a establecer la valoración en base a la probabilidad de ocurrencia y el impacto.

Leyenda de Probabilidad, se establece los niveles de probabilidad de acuerdo a los casos presentados en año, para cada escenario, siendo de nivel muy alto, aquellos que tienen más de 11 casos al año o más de un caso al mes.

Tabla 3
Leyenda de probabilidad

Probabilidad	Detalle	Nivel
P1	Se podría presentar hasta 1 caso al año	1.1 Muy bajo
P2	Se podría presentar de 2 a 4 casos al año	1.2 Bajo
P3	Se podría presentar de 5 a 7 casos al año	1.3 Medio
P4	Se podría presentar de 8 a 11 casos al año	1.4 Alto
P5	Más de 11 casos al año o más de 1 caso al mes	1.5 Muy Alto

Leyenda de Impacto, se establece los niveles de impacto de acuerdo a las pérdidas financieras que tiene las empresas, siendo de nivel muy alto, aquello que tiene pérdidas mayores a \$240,000 al año.

Tabla 4
Leyenda de impacto

Impacto	Detalle	Nivel
I1	Pérdida menor o igual a US\$ 36,000 al año	1.1 Muy bajo
I2	Pérdida mayor a US\$ 36,000 y menor o igual a US\$ 60,000 al año	1.2 Bajo
I3	Pérdida mayor a US\$ 60,000 y menor o igual a US\$120,000 al año	1.3 Medio
I4	Pérdida mayor a US\$ 120,000 y menor o igual a US\$ 240,000 al año	1.4 Alto
I5	Pérdida mayor a US\$ 240,000 al año	1.5 Muy Alto

La clasificación y valoración de los riesgos identificados de acuerdo a los niveles de probabilidad e impacto son los siguientes.

Tabla 5
Clasificación y valoración de los riesgos

Cod.	Clasificación		Valoración del riesgo				
	Factor de Riesgo	Tipo de Evento	Detalle Probabilidad	Nivel de Probabilidad	Detalle del Impacto	Nivel de Impacto	Nivel de Riesgo
R1	4.Eventos Externos	5.Daños a activos materiales	1.2.Bajo	P1	1.2 Bajo	I2	Moderado
R2	4.Eventos Externos	5.Daños a activos materiales	1.1.Muy Bajo	P2	1.5 Muy Alto	I5	Extremo
R3	3.Tecnología	6.Interrupción del Negocio / fallo en el sistema	1.3.Medio	P3	1.4 Alto	I4	Extremo
R4	2.Personas	7.Ejecución entrega y gestión de procesos	1.3.Medio	P3	1.5 Muy Alto	I5	Extremo
R5	4.Eventos Externos	6.Interrupción del Negocio / fallo en el sistema	1.3.Medio	P3	1.5 Muy Alto	I5	Extremo
R6	4.Eventos Externos	6.Interrupción del Negocio / fallo en el sistema	1.1.Muy Bajo	P1	1.5 Muy Alto	I5	Extremo

Los riesgos identificados se ubican en el Mapa de Riesgos de la siguiente manera.

Tabla 6
Mapa de Riesgos

PROBABILIDAD	P.5	MODERADO	EXTREMO	EXTREMO	EXTREMO	EXTREMO
	P.4	MODERADO	ALTO	EXTREMO	EXTREMO	EXTREMO
	P.3	MODERADO	ALTO	EXTREMO	EXTREMO (R4)	EXTREMO (R5, R3)
	P.2	BAJO	MODERADO (R1)	ALTO	EXTREMO	EXTREMO (R2)
	P.1	BAJO	BAJO	MODERADO	ALTO	EXTREMO (R6)
		I.1	I.2	I.3	I.4	I.5
		IMPACTO				

Identificado los escenarios de riesgos junto con su valoración de probabilidad por impacto se debe iniciar con el análisis de impacto de negocio que se describe a continuación.

3.3 Diseño del análisis de impacto de negocio

El factor tiempo se muestra como un factor crucial en cualquier escenario de recuperación ante interrupciones y debe ser determinado de forma particular para cada organización y actividad dentro de la misma. Mientras en algunos escenarios y/o actividades podríamos soportar tiempos de más de un día de interrupción, en el sector bancario, por ejemplo esto podría suponer el cierre definitivo de operaciones. El análisis del impacto en el negocio debe ser desarrollado mediante entrevistas con cada responsable de las principales actividades de riesgo en la empresa, complementada con talleres de formación y sensibilización sobre las actividades de la continuidad del negocio, procurando mostrar de forma práctica como realizar el análisis BIA. El siguiente paso es determinar las actividades críticas y realizar el análisis de impacto de incidencias poniéndonos en el peor de los casos posibles que tenga en cuenta toda la infraestructura necesaria para el desarrollo de la actividad.

Para organizar una correcta recolección de información deberemos construir un sistema de evaluación sistemático con escalas de tiempo y evaluación cualitativa y cuantitativa del impacto que nos permitan posteriormente establecer los criterios adecuados

En este sentido, se debe tener en cuenta toda la infraestructura y servicios necesarios versus su impacto en los clientes tanto internos como externos.

La metodología empleada para definir los procesos críticos de negocio será mediante cuestionario completado en entrevistas con los principales representantes de negocios de las diferentes áreas. El cuestionario empleado tendrá las siguientes preguntas.

- ¿El sub proceso forma parte de los procesos claves para la organización?
- ¿La salida de este Sub-proceso es un input crítico para otro proceso?
- ¿A qué proceso alimenta?
- Si el proceso se interrumpe por 4 horas, ¿Existe una sanción Interna?
- Si el proceso se interrumpe por 8 horas, ¿Existe una sanción Interna?
- Si el proceso se interrumpe, indique el periodo de tiempo a partir del cual el Regulador podría aplicar una sanción, observación o amonestación a la organización por el incumplimiento del proceso.
- Si el proceso se interrumpe, indique el periodo de tiempo en el cual podrían haber multas del corporativo.
- Si el proceso se interrumpe, indique el periodo de tiempo en el que:
 - Organización pierda la oportunidad de cobrar facturas.
 - La organización pierda la oportunidad de captar operaciones (matriculas).
 - La organización pierda la oportunidad de captar alumnos.
- ¿Cuál es el tiempo máximo en el que el proceso debería ser recuperado para no causar un impacto significativo en el nivel de servicio al cliente (interno/externo)?
- ¿Cuál es el número de clientes externos/internos afectados diariamente por la interrupción del proceso?
- ¿Cómo reaccionarían los clientes, el sector universitario y el público en general ante la interrupción del proceso?
- Si el proceso se interrumpe, ¿Cuál sería el impacto en otros procesos o áreas?
- Si el proceso se interrumpe, indique la cantidad de personas potencialmente afectadas por algún daño físico.
- ¿El proceso cuenta con proveedores externos?
- Describir la participación de los proveedores externos en la ejecución del proceso.

A continuación se muestra un ejemplo de los cuestionarios aplicados, en este caso para el proceso de MATRICULA por cada subproceso evaluado.

Tabla 7
Cuestionario aplicado al proceso de Matricula

SUB-PROCESOS EVALUADOS EN EL SERVICIO DE MATRICULA			DEFINICIÓN DE CURRICULA	PROGRAMACIÓN DE HORARIOS	CIERRE DEL CICLO ANTERIOR	FACTURACIÓN - COBRANZA	NUEVOS INGRESOS - ADMISIÓN	MATRICULA	
INFORMACIÓN DEL SUBPROCESO	¿El sub proceso forma parte de los procesos claves para la organización?		SI	SI	SI	SI	SI	SI	
	¿La salida de este Sub-proceso es un input crítico para otro proceso?		SI	SI	SI	SI	SI	SI	
	¿A qué proceso alimenta?		Programación de Horarios	PAGOS PLANILLA DOCENTE	BECAS DE FINICION DE HORARIOS MATRICULA	MATRICULA	MATRICULA PROGRAMACIÓN DE HORARIOS	PROGRAMACIÓN DE HORARIOS	
EVALUACIÓN DE IMPACTO	Impacto Regulatorio (regulación a nivel de grupo)								
	1	Si el proceso se interrumpe por 4 horas, ¿Hay reclamos de Áreas Internas?		NO	NO	NO	SI	NO	SI
	2	Si el proceso se interrumpe por 8 horas, ¿Hay reclamos de Áreas Internas?		NO	NO	NO	SI	NO	SI
	3	Si el proceso se interrumpe, indique el periodo de tiempo a partir del cual el Regulador podría aplicar una sanción, observación o amonestación a la organización por el incumplimiento del proceso. MINEDU, Indecopi u otro organismo regulador del sector Universitario.		<=7 DIAS	<=7 DIAS	<=7 DIAS	<=4 HORAS	NO APLICA	<= 24 HORAS
	4	Si el proceso se interrumpe, indique el periodo de tiempo en el cual podrían haber observaciones, amonestaciones o reclamos del corporativo (Laureate)		<=7 DIAS	<=7 DIAS	<=7 DIAS	<=8 HORAS	<=24 HORAS	<=72 HORAS
	Impacto Financiero								
	5	Si el proces o se interrumpe,	La organización pierda la oportunidad de cobrar facturas por un monto que supere los \$100,000 Dólares americanos.	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	<=72 HORAS
6	indique el periodo de tiempo	La organización pierda la oportunidad de captar operaciones (matriculas) por un monto que supere los \$100,000 Dólares americanos.	NO APLICA	NO APLICA	NO APLICA	<=24 HORAS	<=24 HORAS	<=72 HORAS	
7	en el que:	La organización pierda la oportunidad de captar alumnos en un futuro por un	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	NO APLICA	

		monto que supere los \$100,000 Dólares americanos.					
Impacto en el Servicio al Cliente							
8	¿Cuál es el tiempo máximo en el que el proceso debería ser recuperado para no causar un impacto significativo en el nivel de servicio al cliente (interno/externo)?	<=72 HORAS	<=8 HORAS	<=24 HORAS	<=72 HORAS	<=24 HORAS	<=8 HORAS
9	¿Cuál es el número de clientes externos/internos afectados diariamente por la interrupción del proceso?	> 5000	> 5000	> 5000	> 5000	> 5000	> 5000
Impacto en la Reputación							
10	¿Cómo reaccionarían los clientes, el sector universitario y el público en general ante la interrupción del proceso?	ALTO	MUY ALTO	MUY ALTO	ALTO	ALTO	ALTO
Impacto Operacional							
11	Si el proceso se interrumpe, ¿Cuál sería el impacto en otros procesos o áreas?	MEDIO	MEDIO	ALTO	MUY ALTO	ALTO	ALTO
Daños al Personal							
12	Si el proceso se interrumpe, indique la cantidad de personas potencialmente afectadas por algún daño físico. (Muerte, Lesión o heridas físicas)	SIN DAÑOS	SIN DAÑOS	SIN DAÑOS	SIN DAÑOS	SIN DAÑOS	SIN DAÑOS
Proveedores Externos							
13	¿El proceso cuenta con proveedores externos?	SI	SI	SI	SI	NO	SI
14	Describir la participación de los proveedores externos en la ejecución del proceso	ALTO	ALTO	ALTO	ALTO	NO APLICA	MEDIO
RESULTADO	Prioridad de Recuperación	Nivel-5	Nivel-5	Nivel-5	Nivel-2	Nivel-4	Nivel-2
	Máximo Tiempo Tolerable de Interrupción (MTPD)	<= 7 Días	<= 7 Días	<= 7 Días	<= 8 Horas	<= 48 Horas	<= 8 Horas
	Clasificación del Proceso	Criticidad Media	Criticidad Media	Criticidad Media	Criticidad Alta	Criticidad Media	Criticidad Alta

El objetivo del BIA es comunicar el resultado del Análisis de Impacto de Negocio realizado para los procesos considerados críticos para la entidad educativa superior del sector privado, en función a los procesos evaluados en cada una de las áreas de negocio.

El alcance del BIA deberá ser para las siguientes áreas de negocio que componen el núcleo de la organización.

Tabla 8
Listado de áreas de negocio

AREA
DIRECCION DE ADMISION
VICERECTORADO DE PLANEAMIENTO Y DESARROLLO
VICEPRESIDENCIA DE FINANZAS Y ADMINISTRACION
DIRECCION DE INTELIGENCIA E INNONVACION DIGITAL
VICERRECTORADO DE SERVICIOS UNIVERSITARIOS GESTION DEL CONOCIMIENTO
GESTION DEL CONOCIMIENTO – SERVICIOS DE IMPRESIÓN
DIRECCION DE SERVICIO Y CALIDAD INSTITUCIONAL
VICERECTORADO DE SERVICIOS UNIVERSITARIOS

3.4 Elaboración de BIA

En esta etapa se ejecutó el Análisis de Impacto de Negocio el cual se había planificado en el punto anterior por medio de las entrevistas personales con los Responsables de las Áreas de las diferentes unidades organizativas de la entidad educativa superior del sector privado se realizó lo siguiente.

- Identificación de los procesos ejecutados dentro de las diferentes áreas.
- Evaluación de cada uno de los procesos identificados en base a los factores considerados para evaluar el impacto en la organización, dando como resultado una clasificación para cada uno de los procesos de acuerdo a la Tabla de Clasificación de los procesos evaluados.
- Envío de los resultados preliminares BIA a los responsables de las diferentes áreas.

Tabla 9

Factores considerados para evaluar el impacto

CATEGORÍA	IMPACTO A EVALUAR	PONDERACIÓN
Estratégico	Alineación a objetivos estratégicos	20 %
Regulatorio	Exigencias de la corporación	5 %
	Exigencias y controles internos y externos	5 %
Financiero	Cobrar Facturas	5 %
	Captar Operaciones	5 %
	Captar Alumnos	10 %
Servicio al Cliente	Tiempo Tolerable de Atención al Cliente	15 %
	Número de Clientes Afectados	10 %
Reputación	Daños a la Reputación	5 %
Operación	Impacto Operacional	10 %
Daños a las personas	Daños al personal o público en general	10 %
Total		100 %

La clasificación de los procesos evaluados se ha calculado en base a los resultados de los cuestionarios aplicados, como se mostró en el punto anterior.

Tabla 10

Clasificación de los procesos evaluados

PRIORIDAD DE RECUPERACION	MAXIMO TIEMPO TOLERABLE DE INTERRUPCION (MTPD)	CLASIFICACION DE PROCESO	% IMPACTO EN LA ORGANIZACIÓN
NIVEL 1	<= 4 Horas	Criticidad Alta	> 93%
NIVEL 2	4 - 8 Horas	Criticidad Alta	88% - 93%
NIVEL 3	8 - 24 Horas	Criticidad Alta	81% - 87%
NIVEL 4	24 - 48 Horas	Criticidad Media	65% - 80%
NIVEL 5	48 Horas - 7 Días	Criticidad Media	49% - 64%
NIVEL 6	7 Días - 14 Días	Criticidad Media	33% - 48%
NIVEL 7	14 Días - 30 Días	Criticidad Baja	17% - 32%
NIVEL 8	> 30 Días	Criticidad Baja	0% - 16%

El mapa de procesos y subprocesos de la organización es el siguiente.

Tabla 11

Mapa de procesos de la organización

Del mapa de macro procesos, los evaluados por el Análisis de Impacto de Negocio fueron los siguientes.

Tabla 12

Listado de procesos evaluados

Proceso	Descripción	Área
Admisión Seguimiento	Este proceso comprende la llamada a través de Contact Center de posibles postulantes y su seguimiento para concretar su postulación.	DIRECCIÓN DE ADMISIÓN
Admisión	Este proceso comprende la validación de los requisitos, ejecución de exámenes, evaluación, y emisión de resultados.	DIRECCIÓN DE ADMISIÓN
Matrícula	Este proceso comprende la inscripción, y el registro del postulante admitido como alumno.	VICERECTORADO DE PLANEAMIENTO Y DESARROLLO
Finanzas	Este proceso comprende la facturación de los servicios que brinda la universidad.	VICEPRESIDENCIA DE FINANZAS Y ADMINISTRACION

Inteligencia de Negocio	Este proceso tiene que ver con la transformación de los datos en información de manera que pueda ser usada para la toma de decisiones.	DIRECCIÓN DE INTELIGENCIA E INNOVACIÓN DIGITAL
Biblioteca Aleph	Este proceso comprende el registro del nuevo material bibliográfico en el sistema de Biblioteca Aleph y la gestión de los préstamos de este material a los alumnos, profesores y otros usuarios.	GESTIÓN DEL CONOCIMIENTO
CRM	Este proceso comprende la gestión de la relación con los alumnos.	DIRECCIÓN DE INTELIGENCIA E INNOVACIÓN DIGITAL
Seguridad de la información	Este proceso comprende la gestión y operación de la seguridad de la información.	DIRECCIÓN DE INTELIGENCIA E INNOVACIÓN DIGITAL
Soporte de TI	Este proceso comprende la gestión de requerimientos e incidentes relacionados a tecnologías de la información	DIRECCIÓN DE INTELIGENCIA E INNOVACIÓN DIGITAL
Servicios de TI	Este proceso comprende la entrega de servicios de tecnologías de la información	DIRECCIÓN DE INTELIGENCIA E INNOVACIÓN DIGITAL
Seguridad Física	Este proceso comprende la gestión de la seguridad de infraestructura de la universidad.	DIRECCION DE SERVICIO Y CALIDAD INSTITUCIONAL
Mantenimiento de Infraestructura	Este proceso comprende la identificación, planeamiento y ejecución del mantenimiento de la infraestructura y mobiliario de la universidad.	DIRECCION DE SERVICIO Y CALIDAD INSTITUCIONAL
Virtualización	Este proceso tiene que ver con la difusión, capacitación en la TIC (Tecnologías de la Información y Comunicación) para ser usadas en el diseño e implementación de los cursos presenciales, blended u online	VICERRECTORADO DE SERVICIOS UNIVERSITARIOS

Como resultado de aplicar el Análisis de Impacto de Negocio a los diferentes procesos de las áreas entrevistadas, se obtuvo la siguiente clasificación.

Tabla 13
Sub procesos con criticidad alta

Sub Procesos	Prioridad de Recuperación	Máximo Tiempo Tolerable de Interrupción (MTPD)	Clasificación del Subproceso	RTO Estimado
Evaluación / incorporación	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Telemarketing	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Gestión de multicanales	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Facturación	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Cobranza	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Matricula	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Crm	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Mantenimiento de infraestructura	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Cursos blended	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Cursos full	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Soporte de aplicaciones académicas	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 Horas
Soporte de aplicaciones financieras	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 Horas
Servicios de ti (soporte)	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 Horas

Tabla 14
Sub procesos con criticidad media

Sub Procesos	Prioridad de Recuperación	Máximo Tiempo Tolerable de Interrupción (MTPD)	Clasificación del Subproceso	RTO Estimado
Prospección	Nivel-6	<= 14 Días	Criticidad Media	< 10 Días
Seguimiento – Cierre	Nivel-6	<= 14 Días	Criticidad Media	< 10 Días
Definición de Curricula	Nivel-5	<= 7 Días	Criticidad Media	< 5 Días
Programación de Horarios	Nivel-5	<= 7 Días	Criticidad Media	< 5 Días
Cierre del ciclo anterior	Nivel-5	<= 7 Días	Criticidad Media	< 5 Días
Nuevos ingresos - Admisión	Nivel-4	<= 48 Horas	Criticidad Media	< 24 horas
Becas y Créditos	Nivel-6	<= 14 Días	Criticidad Media	< 10 Días
Monitoreo y cumplimiento de políticas	Nivel-6	<= 14 Días	Criticidad Media	< 10 Días
Administración de accesos	Nivel-4	<= 48 Horas	Criticidad Media	< 24 horas
Gestión de Incidentes de Seguridad de Información	Nivel-4	<= 48 Horas	Criticidad Media	< 24 horas
Seguridad Física – Control Patrimonial	Nivel-5	<= 7 Días	Criticidad Media	< 72 horas
Sistema de Salud en el Trabajo	Nivel-6	<= 14 Días	Criticidad Media	< 07 Días

Tabla 15
Sub procesos con criticidad baja

Sub Procesos	Prioridad de Recuperación	Máximo Tiempo Tolerable de Interrupción (MTPD)	Clasificación del Subproceso	RTO Estimado
Políticas – reglamento	Nivel-7	<= 30 Días	Criticidad Baja	< 15 Días
Trámites	Nivel-7	<= 30 Días	Criticidad Baja	< 15 Días
BI	Nivel-7	<= 30 Días	Criticidad Baja	< 15 Días
Carga de información	Nivel-8	>30 Días	Criticidad Baja	<20 Días
Biblioteca Aleph	Nivel-7	<= 30 Días	Criticidad Baja	< 15 Días
Aseguramiento y control de calidad	Nivel-7	<= 30 Días	Criticidad Baja	< 15 Días

De los subprocesos analizados se obtiene como resultado que el 42% se ha clasificado con nivel de criticidad ALTO por los propietarios del proceso, el 39% con criticidad MEDIA y el 19% con criticidad BAJA.

Figura 15. Clasificación de los Sub-Procesos

3.5 Estructura de desglose de trabajo

La estructura de desglose de trabajo del proyecto de ejecución de DRP es el siguiente.

3.6 Estrategias de DRP

A nivel de infraestructura, personal, recursos, proveedores críticos y registros vitales, se debe tomar en consideración la seguridad del personal, de la información y sitios alternos de operaciones.

Existen diferentes alternativas de recuperación donde la estrategia apropiada es la que tiene un costo para un tiempo aceptable de recuperación que también es razonable con el impacto y la probabilidad de ocurrencia. Las acciones más efectivas serían:

- Eliminar la amenaza completamente.
- Minimizar la probabilidad y el efecto de la ocurrencia.

Una estrategia de recuperación es una combinación de medidas preventivas, detectivas y correctivas. La selección de una estrategia de recuperación depende de:

- La criticidad del proceso del negocio y las aplicaciones que soportan los procesos.
- Costo.
- El tiempo requerido para recuperarse.
- Seguridad.

En general, cada plataforma TI en la que corra una aplicación que soporte una función crítica del negocio necesitará una estrategia de recuperación.

Las interrupciones más prolongadas y más costosas, en particular los desastres que afectan la instalación física primaria del centro de cómputo, requieren alternativas de recuperación en un sitio distinto a la ubicación primaria (offsite). Los tipos de instalaciones de respaldo de hardware en sitio alternativo que existen son:

Mirror Site: Es un sitio alternativo que contiene una réplica exacta de otro. Estas réplicas u espejos se suelen crear para facilitar descargas grandes y facilitar el acceso a la información aun cuando haya fallos en el servicio del servidor principal.

Los espejos suelen sincronizarse periódicamente con el servidor principal para mantener la integridad de la información. En el caso de las redes, mirror también hace referencia al modo en el que trabaja un switch, al hacer réplica de todos los paquetes que este conmuta direccionados a un solo puerto a través del cual, con un analizador de tráfico, se puede observar todo el tráfico de la red.

Hot-Site: Se configuran totalmente y están listos para operar dentro de varias horas. El equipo, red y software del sistema deben ser compatibles con la instalación que está siendo respaldada. Las únicas necesidades adicionales son personal, programas, archivos de datos y documentación. Los costos asociados con el uso de un hot site de terceros por lo general son elevados, pero más bajos que crear un sitio redundante y con frecuencia son costos justificables para aplicaciones críticas. El hot site está destinado para operaciones de emergencia durante un período limitado de tiempo y no para uso prolongado.

Recuperación inmediata; el sitio alternativo requiere de soluciones de replicación tanto a nivel de infraestructura como de datos (0-4 horas).

Warm-Side: Están en parte configurados, por lo general con conexiones de red y equipo periférico seleccionado, como por ejemplo, unidades de discos y otros controladores, pero sin la computadora principal. Algunas veces un warm site está equipado con una CPU menos potente que la que se usa generalmente. El supuesto detrás del concepto warm site es que la computadora puede por lo general obtenerse rápidamente para una instalación de emergencia y como la computadora es la unidad más cara, dicho acuerdo es menos costoso que un hot site.

Recuperación basada en copias de respaldo; el Sitio Alternativo debe existir con conectividad, enlaces de terceros y equipos listos para restaurar las copias de respaldo (24 a 48 horas).

Cold-Side: Es el menos costoso de sitio de copia de seguridad de una organización para operar. No incluye la respaldada copia de los datos y la información de la ubicación original de la organización, ni tampoco incluye hardware ya configurado. La falta de hardware provisionado contribuye a los costos mínimos de puesta en marcha del cold sites, pero requiere tiempo adicional tras el desastre de tener la operación funcionando a una capacidad cercana a los que antes de la catástrofe. En algunos casos, cold sites puede tener equipo disponible, pero no es operacional

Recuperación basada en copias de respaldo; el Sitio Alternativo debe existir con por lo menos la conectividad necesaria (1 semana).

Acuerdos Interinstitucionales: Este es un método es poco frecuente, ya que consiste en que entre dos o más organizaciones cuenten con equipos o aplicaciones similares para que en el momento de un desastre se pueda subir los servicios. Bajo el acuerdo típico, los participantes prometen proveerse mutuamente tiempos de computadoras cuando surja una emergencia.

Este sitio alternativo debe ubicarse lejanamente de la instalación del sistema principal y evitar que ambos fallen por estar en el mismo sector, ya sea por apagón, terremoto, ataque violento o vía Internet, entre otras.

El hardware y el software deben ser absolutamente compatibles para subir los servicios para el adecuado funcionamiento. Los recursos en ambas instalaciones deben ser iguales por lo que las revisiones periódicas y pruebas periódicas son básicas.

Figura 16. Estrategias de continuidad y recuperación costo vs. Tiempo

3.7 Matriz de estrategias

A continuación se presenta la Matriz de estrategias en función del costo, equipamiento y tiempo de configuración.

Tabla 16
Matriz de Estrategias

TIPO DE SITIO ALTERNO	COSTO	EQUIPAMIENTO DE HARDWARE	COMUNICACIÓN	TIEMPO CONFIGURACIÓN	SITIO
COLD	Bajo	Ninguno	Ninguno	Largo Entre 24 y 72 horas	Centro de Computo Alterno
WARM	Medio	Parcial	Parcial / Completo	Medio Entre 8 y 24 horas	Centro de Computo Alterno / Nube
HOT	Alto	Completo	Completo	Corto Entre 4 y 8 horas	Centro de Computo alternativo / Nube
MIRROR	Muy Alto	Completo	Completo	Ninguno 0 horas	Centro de Computo Alterno / Cloud

De acuerdo a la matriz de estrategias presentadas en el cuadro anterior y evaluando que se necesita un equipamiento completo de Hardware, el sistema de comunicación debe estar completo y disponible en todo momento, considerando que el tiempo de configuración será muy corto y que se requiere de un centro de cómputo alterno de manera física o en la nube, se ha decidido optar por la estrategia de HOT SITE para la recuperación del centro de cómputo de la universidad.

Tabla 17
Matriz de alternativas de solución por estrategia

Tipo	Alternativas de Solución	Tipo de Alternativas	Implementador
HOT SITE	Local propio	Implementación de site alterno con infraestructura propia	Personal interno en San Isidro. Personal de interno en Sede Villa.
	Hosting	DC externo con infraestructura equipada en local de proveedor	<u>Proveedores</u> ITG SOLUTIONS. CLARO. NET SECURE. IBM LEVEL3
	Cloud	DC en nube	<u>Proveedores</u> AZURE AMAZON IBM
MIRROR SITE	Local	Replicación directa hacia el data center externo.	<u>Proveedores</u> ITG SOLUTIONS. CLARO. NET SECURE. IBM LEVEL3
	Cloud	Replicación a data center en nube	<u>Proveedores</u> AZURE AMAZON IBM VMWARE (DRaaS)

La organización cuenta con un centro de cómputo alterno, así como infraestructura propia para soportar los procesos críticos de negocio; es por ello, de las alternativas de solución que se plantea se elige el Local Propio, con esta alternativa la universidad ahorrará costos al no tener que invertir en equipamiento.

La sede seleccionada para la implantación del DRP será la sede San Isidro. En un futuro no muy lejano es probable que se pueda migrar al tipo de configuración MIRROR SITE.

En resumen, se presenta la siguiente tabla de objetivos específicos y requerimientos.

Tabla 18

Resumen de objetivos específicos y requerimientos

TABLA RESUMEN DE OBJETIVOS ESPECIFICOS Y REQUERIMIENTOS		
OBJETIVO ESPECIFICO	REQUERIMIENTO	DESCRIPCION
Realizar un Análisis de Riesgos que permita determinar los escenarios de amenazas que podrían afectar al centro de cómputo.	5.2.Compromiso de la gerencia	Asegurar compatibilidad con la dirección estratégica de la organización.
	6.1. Acciones a atender, riesgos y oportunidades.	Determinar riesgos y oportunidades para asegurar que el sistema gerencial alcance sus resultados, prevenir efectos indeseables.
	6.2. Objetivos de continuidad de negocio y planes para alcanzarlos.	La alta dirección debe asegurarse que los objetivos están establecidos para funciones relevantes y niveles de la organización.
	8.2.3. Evaluación de riesgos	Analizar sistemáticamente el riesgo, evaluar que interrupción relacionada con qué riesgo requiere tratamiento, identifica riesgos conmensurables.
Desarrollar un Análisis de Impacto al Negocio (BIA), que permita determinar el impacto operacional, económico, que podría tener la universidad como resultado de la ocurrencia de una interrupción o desastre.	4.2. Entendimiento de las necesidades y expectativas de las partes interesadas.	La organización determina las partes interesadas relevantes y sus necesidades y requerimientos.
	4.3.2. Alcance del SGCN.	Establece las partes de la organización que deben ser incluidas, identifica productos y servicios relacionados con el alcance del SGCN.
	5.2.Compromiso de la gerencia	Asegurar compatibilidad con la dirección estratégica de la organización.
	8.2.1.a Establecer el contexto de la evaluación, definir criterios y evaluar el potencial impacto relacionado a un incidente alterador.	Establecer, implementar y mantener un proceso documentado y formal para el análisis del impacto de negocio y evaluación del riesgo.
	8.2.1.b Tomar en consideración requerimientos legales y otros a los cuales la organización está suscrita.	Establecer, implementar y mantener un proceso documentado y formal para el análisis del impacto de negocio y evaluación del riesgo.

	8.2.2. Análisis del Impacto	Identificación de actividades que apoyan la provisión de productos y servicios.
Definir las estrategias de recuperación de desastres de TI que permitirán cumplir con los objetivos de recuperación establecidos por el centro de cómputo.	5.3 Política	La alta gerencia debe establecer y comunicar la política de continuidad del negocio
	7.5.3 Control de información documentada.	Información documentada, disponible y adecuadamente protegida.
	8.3.1. Determinación y selección de estrategias	Debe determinar apropiadas opciones para proteger actividades priorizadas, estabilizar las dependencias y recursos de apoyo, mitigar y gestionar impactos.
	8.3.3. Protección y mitigación	Riesgos identificados que requieren tratamiento, deben considerar medidas proactivas que reduzcan la probabilidad de interrupción.
Definir las alternativas de solución de recuperación para cada estrategia.	8.4.2. Estructura de respuesta	Identifica los impactos que pudiesen identificar la iniciación de una respuesta formal.
	8.4.3. Aviso y comunicación	Establecer, implementar y mantener procedimientos para detección y monitoreo de incidente, comunicación interna en la organización, asegurar disponibilidad de medios de comunicación, registro de información vital sobre el incidente.
	8.4.4 Planes de continuidad del negocio	Roles y responsabilidades definidas para personas y equipos que tienen autoridad, activación de respuesta, gestión de consecuencias.
	8.4.5 Recuperación	Documentar procedimientos para restablecer y retornar las actividades del negocio después de un incidente.
	8.5. Ejercicio y ensayo	Ejercitar y ensayar sus procedimientos de continuidad para asegurar que son consistentes con los objetivos del SGCN.

4 DISEÑO DE LA SOLUCION

4.1 Declaración de política de continuidad de negocio

La política global de continuidad de negocio que se implantará, publicará y difundirá en la organización contemplando los siguientes acuerdos.

ALCANCE: Esta política aplica para todo el personal que labore en la entidad educativa superior del sector privado con el fin de garantizar la continuidad de negocio, en caso de un evento que afecte la operación normal.

INTRODUCCION: La política de continuidad de negocio tiene como objetivo proteger los procesos críticos del negocio, contra desastres o fallas mayores, junto con las posibles consecuencias que se puedan tener, como pérdidas de tipo financiero, credibilidad, productividad, etc. debido a la no disponibilidad de los recursos de la organización. El Plan de Recuperación de Desastres, busca mitigar el riesgo a dichas fallas o desastres, mediante un plan que permita la pronta recuperación de la operación, en caso de presentarse algún evento que afecte el flujo normal de las actividades de la universidad.

OBJETIVO: Evitar interrupciones a los procesos críticos del negocio como consecuencia de fallas o desastres.

ENUNCIADO DE LA POLÍTICA GENERAL: Debido a que cualquier interrupción en los procesos de negocio afecta a la operación, es responsabilidad de las directivas de la organización aprobar un Plan de Recuperación de Desastres, que cubra las actividades esenciales y críticas de la entidad educativa superior del sector privado, así como garantizar la operación de todos los procesos vitales para la organización que son soportados por el área tecnológica.

POLITICAS RELACIONADAS: Políticas de respaldo y restauración, Política de Seguridad Física de Data Center.

ROLES Y RESPONSABILIDADES: Esta política debe ser aprobada por las directivas de la organización, luego del estudio previo y detallado de sus posibles consecuencias, con el fin de garantizar la continuidad de negocio en caso de un evento que afecte la operación normal de los procesos críticos que son soportados por el área tecnológica.

SANCIONES: En este caso especial, si las directivas de la organización se comprometen a desarrollar el plan, será responsabilidad de ellos, no faltar a este compromiso y tener en

cuenta que al no realizar dicho plan, la compañía pudiera estar expuesta a procesos legales y contractuales, que pudieran poner en riesgo el futuro de la operación de la entidad educativa.

REVISION DE LA POLITICA: Esta política debe ser modificada si existieran cambios en los procesos de negocio de la organización o en su infraestructura tecnológica, de no haber cambios, se debe realizar su revisión anualmente.

4.2 Elaboración de DRP

ESTRUCTURA ORGANIZACIONAL

Define los equipos de trabajo involucrados en el esfuerzo de la recuperación de los servicios brindados por la Sala de Servidores en caso de contingencia y sus responsabilidades asociadas. Las responsabilidades se desglosan en categorías de antes, durante y después de la contingencia.

Se muestra un listado con los integrantes de los equipos y sus números telefónicos en las oficinas, de su casa y cualquier otro teléfono alternativo para su localización. La organización para la recuperación es la siguiente.

Figura 17. Estructura Organizacional de DRP

A continuación, se muestra la interacción de los equipos y sus integrantes, es importante recalcar que la organización también debe formar parte del plan general de BCP.

Tabla 19
Miembros de cada grupo de recuperación

EQUIPO GERENCIAL	Director de TI – Líder Principal Jefe IPTI – Líder Alterno		
EQUIPO COORDINADOR	Jefe de STI – Líder Principal		
	Jefe de IPTI – Líder Alterno	Director de Sec. Académica	Jefe de Tice
	Director de RRHH	Gerente de SI	Director Ejecutivo
	Director de DI	Vicerrector Administrativo	Vicerrectora de Marketing
	Director de Admisión	Vicerrector Académico	Vicepresidencia de Finanzas y Administración
	Director EPG	Jefe de CDI	
EQUIPO USUARIO	Jefe IPTI – Líder Principal	Coordinador de Plataforma – Líder Alterno	Coordinador de Redes y Comunicaciones
	Jefe de STI	Coordinador de Gestión de calidad.	Administrador de BBD
	Administrador de Servicios de voz		
EQUIPO APOYO ADMINISTRATIVO	Jefe de IPTI – Líder Principal	Jefe de STI – Líder Alterno	Jefe de Desarrollo de proyectos

Es importante recalcar que el equipo está conformado por los líderes de los equipos de usuarios definidos como parte de los procesos críticos de la organización, esto significa que estos integrantes forman parte del equipo coordinador, siendo al mismo tiempo los líderes de los diferentes grupos de usuarios, estos últimos separados por áreas funcionales.

EQUIPOS DE RECUPERACION

A continuación se detalla los roles de cada grupo de recuperación.

1. Equipo Gerencial	
Coordina con: Equipo Coordinador.	Reporta a: Rectorado
Función Principal	

Declarar la contingencia y tomar decisiones significativas referentes a la implantación del plan de recuperación del negocio para los procesos críticos afectados.
Funciones o Tareas
<p>Previas al Desastre:</p> <p>Conocer y comprender los criterios especificados para la toma de decisiones del plan de recuperación.</p> <p>Revisar y aprobar las decisiones estratégicas sobre políticas de recuperación.</p> <p>Tomar decisiones relativas a problemas financieros y acuerdos contractuales para implantar el plan de recuperación a través de la estrategia definida.</p> <p>Velar para que el plan de recuperación se mantenga actualizado y operativo.</p> <p>Aprobar la conformación de los equipos que tendrán participación activa en la organización de respuesta a contingencias, señalando sus roles y funciones.</p> <p>Aprobar la ubicación y tipo de Centro de Procesamiento de Respaldo CA adecuado para la entidad educativa del sector privado.</p>
<p>Durante el Desastre:</p> <p>Decidir la “Declaración oficial de contingencia”, activar el plan de recuperación y comunicar a la Región la ocurrencia del Incidente.</p> <p>Proveer guías corporativas al equipo coordinador.</p> <p>Mantener informada a la Región del estado de la recuperación.</p> <p>Mantener contacto con las autoridades (Ejército, Policía, Bomberos, INDECI, etc.) en la medida que sea requerido.</p> <p>Aprobar/rechazar negociaciones financieras para la recuperación.</p> <p>Autorizar el retorno al centro primario.</p> <p>Brindar la información oficial de la contingencia a los usuarios y los tiempos estimados de reposición de operaciones para ser informados a los clientes del servicio (usuarios) de la universidad.</p> <p>Supervisar el registro oportuno de incidentes, contingencias y/o desastres en la Bitácora de Contingencias.</p>

<p>Posterior al Desastre:</p> <p>Velar por la actualización del plan en caso de haber surgido modificaciones y/o sugerencias de mejoras durante la situación de contingencia.</p> <p>Requerir la verificación del proceso de normalización de las operaciones críticas restauradas las cuales garantizan la continuidad del negocio.</p> <p>Evaluar el resultado de la recuperación y emitir sus recomendaciones.</p> <p>Informar a la Región los resultados sobre lo acontecido.</p>				
Conformación Propuesta (*)				
<p>El Director de TI y el Jefe de IPTI, asumirán dentro de sus funciones, la dirección y coordinación del DRP.</p>				
Integrantes Propuestos (*)				
(Líder)	Nombre	Teléfono		
		Anexo	Domicilio	Celular
Principal	Luis Miguel Velásquez Castañeda	73xx	27542xx	9946113xx
Alternó	William Romero Solís	73xx	25631xx	9975662xx

Los Integrantes deben tener niveles directivos y gerenciales que conozcan la operación de la organización, la estrategia Tecnológica, financiera y los fundamentos de recuperación del negocio. Adicionalmente cabe resaltar que el Líder Alternó del presente plan adicionalmente a sus funciones tiene la función de Líder de Equipo ante la ausencia del líder principal para el manejo de la Crisis.

2. Equipo Coordinador	
Coordina con: Equipo de Sistemas. Equipo de Apoyo Administrativo.	Reporta a: Equipo Gerencial
Función Principal	
<p>Tomar decisiones gerenciales tácticas y operativas necesarias para que los miembros de los equipos de recuperación puedan trabajar sin interrupciones, supervisar a los equipos de recuperación en su tarea operativa y ser responsable por las reparaciones y/o reconstrucción de las localidades afectadas después de la contingencia.</p>	
Funciones o Tareas	
<p>Previas al Desastre:</p> <p>Garantizar el mantenimiento del plan de recuperación.</p> <p>Conocer y comprender los procedimientos para notificar al centro alterno (ver Anexo D)</p> <p>Garantizar y supervisar la actualización permanente del DRP y todos sus procedimientos.</p> <p>Capacitar al personal de la organización, sobre los procedimientos de declaración de contingencia y DRP.</p> <p>Participar en las pruebas y mantenimiento del plan de recuperación.</p> <p>Verificar el cumplimiento de las actividades previas a la contingencia definidas para cada equipo de recuperación</p> <p>Asegurar que los planes y procedimientos para el respaldo y restauración de cualquier aplicación vital estén completos, reflejen los cambios en la plataforma informática y aplicaciones sean validados para su confiabilidad periódicamente, mediante la prueba correspondiente.</p> <p>Trabajar con el Equipo de Sistemas y el Equipo de Apoyo Administrativo para asegurarse que las distintas formas de respaldo estén a salvo y organizadas para una rápida recuperación.</p> <p>Garantizar que el software a ser restaurado ante la ocurrencia de una contingencia funcione correctamente en los equipos de reemplazo.</p> <p>Entrenar periódicamente al personal responsable de los procesos calificados como críticos para ejecutar los procedimientos ante una contingencia.</p>	

Durante el Desastre:				
<p>Definir el nivel de severidad de la contingencia y comunicarla al Equipo Gerencial a efectos de activar o no el plan de contingencia.</p> <p>Notificar y reunir a los equipos de recuperación.</p> <p>Evaluar los daños, estimar el tiempo requerido para la recuperación de los servicios perdidos o afectados e informar al equipo gerencial para la toma de decisión.</p> <p>Asegurar que los equipos estén realizando sus tareas.</p> <p>Encargarse de la autorización de los gastos y pago de facturas para el reemplazo de equipo o suministros.</p> <p>Revisar y supervisar cualquier reemplazo y/o reparación de las instalaciones dañadas.</p> <p>Solicitar al Equipo de Apoyo la recuperación de los respaldos magnéticos y los documentos vitales para contingencia (manuales y procedimientos) que habrán de estar resguardados en lugar seguro fuera del local principal de la universidad.</p>				
Posterior al Desastre:				
<p>Evaluar el desempeño general de los equipos de trabajo durante el proceso de recuperación.</p> <p>Evaluar la efectividad general del plan de recuperación del negocio.</p> <p>Revisar/actualizar los procedimientos existentes.</p> <p>Evaluar la efectividad general del proveedor de centro alterno.</p> <p>Realizar las recomendaciones con respecto al cumplimiento de las funciones asignadas a cada miembro de los equipos con los cuales coordina.</p>				
Conformación Propuesta (*)				
Este equipo estará liderado por el Jefe de STI contando como Back Up al Jefe de IPTI.				
Integrantes Propuestos (*)				
Función	Nombre	Teléfonos		
		Anexo	Domicilio	Celular
Líder	Henry	7340	34409xx	9975562xx
Integrante (Líder Alterno)	William	7350	25631xx	9975662xx
Integrante	Mariana	2100	42148xx	9973775xx
Integrante	Humberto	1020	62263xx	9890489xx 9974488xx
Integrante	Lea	2970	65430xx	9890488xx
Integrante	Milagros	2400		9946113xx

Integrante	Ángel	2920	62421xx	9946164xx
Integrante	Teresa	2140		9866298xx
Integrante	José	2250	34504xx	9975998xx
Integrante	Demetrio	1090		9946113xx
Integrante	Tomás	2390	43746xx	9946113xx
Integrante	Blanca	5100	47503xx	9975662xx 9756535xx
Integrante	Jorge	4100	25554xx	9975662xx 993 232 0xx
Integrante	Oscar	8100	36842xx	9935318xx
Integrante	Guillermo	3100		9444839xx
Integrante	Rodolfo	1100		9890489xx
Integrante	Marysol	7130		

Los Integrantes deben tener niveles gerenciales de las áreas de Informática y de otras áreas de la compañía, con habilidades para coordinar y supervisar equipos de trabajo y con conocimiento de los procedimientos del plan de recuperación.

3. Equipo de Sistemas	
Coordina con:	Reporta a:
Equipo de Apoyo Administrativo	Equipo Coordinador
Función Principal	
Recuperar y restaurar el ambiente operativo de sistemas en lo relacionado con hardware, software, periféricos y comunicaciones en el centro alterno, garantizando el soporte informático al negocio.	
Funciones o Tareas	
<p>Previas al Desastre:</p> <p>Tener un inventario actualizado del equipo de cómputo.</p> <p>Documentar un inventario de registros vitales y los requerimientos mínimos para operar en caso de contingencia.</p> <p>Identificar y documentar los procedimientos de respaldo y recuperación.</p> <p>Mantener actualizado y fuera de las instalaciones de la <i>universidad</i> los elementos críticos necesarios para la recuperación.</p> <p>Conocer la ubicación de la bóveda externa así como el procedimiento para la obtención de los registros vitales.</p> <p>Probar los procedimientos de respaldo/recuperación en la <i>universidad</i> y en el centro alterno.</p> <p>Revisar y analizar los resultados de las pruebas e implantar las modificaciones según sea necesario.</p> <p>Verificar la disponibilidad del centro alterno.</p>	

Durante el Desastre:

Restaurar el ambiente operativo en la localidad alterna de recuperación.

Proporcionar asistencia al usuario final en los sistemas de información según se requiera.

Evaluar el equipo y las instalaciones dañadas para su reparación o reemplazo.

Preparar listas detalladas de los equipos que requieren reparación o reemplazo.

Coordinar los cambios y configuraciones en los equipos de telecomunicaciones.

Contactar a los recursos externos y/o proveedores necesarios para restaurar los servicios y/o procesos afectados por la contingencia, en coordinación con el Equipo de Apoyo Administrativo.

Asegurar que todo el personal de soporte que se requiera ha sido contactado para proveer asistencia.

Ejecutar los procedimientos necesarios en coordinación con el Equipo de Apoyo Administrativo para trasladar los equipos a un nuevo ambiente y de ser necesarios, adquirir otros nuevos.

Una vez que se han trasladado los medios magnéticos al ambiente alternativo, el Equipo de Soporte Técnico debe comenzar la habilitación de los equipos computacionales y de comunicaciones, restauración de los datos y estar listo para realizar otras funciones de acuerdo a la necesidad.

Proponer al Equipo Coordinador los equipos o personas necesarios para el esfuerzo de reposición de cada servicio.

El grupo debe asegurar que todas las instalaciones estén operativas y listas para transmitir y recibir datos desde y hacia el Centro de Procesamiento de Respaldo.

Mantener permanentemente informado al Equipo Coordinador de su actividad y los resultados obtenidos en el esfuerzo de reposición del servicio.

Asegurar que el procesamiento normal pueda llevarse a cabo tan pronto como el sistema, equipos y comunicaciones requeridos, estén disponibles.

Asegurar que cualquier aplicación crítica sea procesada dentro del tiempo establecido.

Comunicar los hechos al Director de IT.

<p>Posterior al Desastre:</p> <p>Evaluar la efectividad del plan de recuperación para su área de responsabilidad.</p> <p>Evaluar la efectividad del equipo de trabajo durante la contingencia.</p> <p>Revisar/actualizar los procedimientos existentes.</p> <p>Modificar las tareas y procedimientos del equipo de trabajo según sea necesario.</p> <p>Informar sobre el impacto del daño.</p>				
<p>Conformación Propuesta (*)</p>				
<p>Este equipo estará integrado por: el personal perteneciente al Área de Sistemas.</p>				
<p>Integrantes Propuestos (*)</p>				
Función	Nombre	Teléfono		
		Anexo	Domicilio	Celular
Líder	Jorge	73xx	9946668xx	9975932xx
Alternativo	Úrsula	73xx	53653xx	9935340xx
Integrante	Jorge	73xx	9972041xx	9975968xx
Integrante	Miguel	77xx	34611xx	9975662xx

4. Equipo de Apoyo Administrativo	
Coordina con:	Reporta a:
Equipo de Sistemas.	Equipo Coordinador.
Función Principal	
Asistir al personal de la universidad , solucionando situaciones de seguridad, control de entradas y salidas de recursos, transporte, daños físicos, pago de nómina así como comunicar el desastre interna y externamente.	
Funciones o Tareas	
<p>Previas al Desastre:</p> <p>Identificar y documentar los requerimientos mínimos de operación, la relación de proveedores con su respectivo contacto y apoyar en el mantenimiento del plan de recuperación.</p> <p>Definir y garantizar la comunicación entre los equipos de recuperación.</p> <p>Participar en las pruebas del plan de recuperación.</p> <p>Definir los comunicados de notificación interna y externa</p>	
<p>Durante el Desastre:</p> <p>Trasladarse en caso necesario, al punto de reunión determinado.</p> <p>Evaluar la disponibilidad del personal crítico.</p> <p>Llamar a los proveedores o consultores profesionales diferentes a los de informática, según sea necesario.</p> <p>Ejecutar los procedimientos de traslado y obtención de los registros vitales, si es necesario</p> <p>Contratar personal temporal en caso de ser necesario.</p> <p>Hacerse cargo del alojamiento, servicios médicos, etc., en el centro alterno.</p> <p>Coordinar la adecuación del Centro de Procesamiento de Respaldo con el mobiliario apropiado y requerido, en caso de una contingencia.</p> <p>Proveer al personal de la universidad facilidades de transporte y equipo.</p> <p>Comunicar números de teléfono y ubicación del Centro de Procesamiento de Respaldo a todos los miembros de los equipos.</p> <p>Brindar cualquier asistencia necesaria al Equipo de Sistemas en el esfuerzo de habilitación del Centro de Procesamiento de Respaldo.</p> <p>Realizar arreglos para gastos tales como, compromisos de pago de servicios en caso de requerirse la intervención de proveedores externos.</p> <p>Mantener al Equipo Coordinador informados de su actividad.</p>	

<p>Posterior al Desastre:</p> <p>Evaluar la efectividad del plan de recuperación para su área de responsabilidad. Revisar/actualizar los procedimientos existentes</p>				
Conformación Propuesta (*)				
Este equipo estará integrado por: la Gerente de Recursos Humanos, personal de compras, finanzas y operaciones, estas personas asumirán dentro de sus funciones, las propias del Equipo de Apoyo Administrativo.				
Integrantes Propuestos (*)				
Función	Nombre	Teléfono		
		Anexo	Domicilio	Celular
Líder	William	7350	25631xx	9975662xx
Alternó	Henry	7340	34409xx	9975662xx
Integrante	Liliana	7330	27526xx	9935260xx
Integrante	Shirley	7360	9998541xx	9975925xx

5. Equipo de Usuarios	
Coordina con:	Reporta a:
Equipo de Apoyo Administrativo.	Equipo Coordinador.
Función Principal	
Mantener o recuperar la operación de la empresa en caso de una contingencia que imposibilite el uso ya sea de la infraestructura física de la empresa como de los sistemas de información de la misma.	
Funciones o Tareas	
<p>Previas al Desastre:</p> <p>Mantener actualizado el Orange Box (Caja de Registros Vitales) con toda la información que los usuarios de su área requerirán para su trabajo diario. Mantener actualizados los Procedimientos de Operación Estándar (SOP).</p>	
<p>Durante el Desastre:</p> <p>Trasladarse en caso necesario, al punto de reunión determinado por el presente plan, salvo comunicación explícita del Equipo de Apoyo Administrativo que indique trasladarse al site alterno 1. Esperar una comunicación oficial por parte del Equipo Gerencial sobre el estado de la contingencia. En caso de trato directo con clientes, sólo comunicar la versión única y oficial de los hechos proporcionada por el Equipo Gerencial e indicar siempre la pronta normalización de operaciones. Recuperar las Orange Box (Caja de Registros Vitales) de sus respectivas áreas para contar con toda la información necesaria para su trabajo en contingencia.</p>	
<p>Posterior al Desastre:</p> <p>Realizar el ingreso manual de la información obtenida durante la contingencia a los sistemas de información. Realizar las labores que el equipo de Gerencia indique para volver a la operación normal.</p>	
Conformación Propuesta (*)	
Este equipo estará integrado por: todo el personal de todas las áreas de <i>la universidad</i> .	

Integrantes Propuestos (*)				
Función	Nombre	Teléfono		
		Anexo	Domicilio	Celular
Líder Principal	William	7350	25631xx	9975662xx
Líder Alterno	Jorge	7353	9946668xx	9975932xx
Integrante	Úrsula	7352	53653xx	9935340xx
Integrante	Jorge	7351	9972041xx	9975968xx
Integrante	Miguel	7777	34611xx	9975662xx
Integrante	Henry Longa Alegría	7340	34409xx	9975662xx
Integrante	Martín Valderrama	7348	56703xx	9946164xx

4.3 EJECUCION DEL PLAN DE RECUPERACION

En caso de ocurrencia de una contingencia, ésta podrá presentarse en diferentes escenarios dentro de la universidad, en cada escenario a su vez existirán diferentes niveles en los cuales podría verse afectado.

Tabla 20
Escenarios de Desastres en la sala de servidores

ESCENARIOS	FUENTES	ACCION
DESASTRE EN LA SALA DE SERVIDORES	PERDIDA DE LA SALA DE SERVIDORES	Activación DRP
	PERDIDA DE EQUIPOS CRITICOS	Activación DRP
	RHO (Controlador de dominio principal administrativo)	
	ADACADMO (Controlador de dominio principal académico)	
	DNSUPC	
	FWUPC-Checkpoint (Seguridad Perimetral Monterrico)	
	FWACADUPC (Seguridad Perimetral Monterrico Acad.)	
	Veritas (Sistema de Backup / Restore)	
	PROD	
	MoodleProd	
	Intranet	
	SPRING	
	SPRINGUPN	
	Upmail1	
	Firewall-IRA	
	Upmail1a	
	ADACADS11 (Controlador de dominio principal administrativo)	
	DHCP-SI (Controlador de dominio principal académico)	
	FWCIB (Seguridad Perimetral San Isidro)	
	FWACAD (Seguridad Perimetral San Isidro Acad.)	
	DNSCIB	
	VERITASSI (Sistema de Backup / Restore)	
	UPCMAIL2	
	UPCMAIL2A	
	PRODSI2	
	IntranetCib	
	FWIRASI	
	AULAVIRTUALSI	
	FW-SN (Seguridad Perimetral)	
	DHCP-SN	
	UPCMAIL3	
	PERDIDA DE EQUIPOS DE COMUNICACIÓN	Activación DRP
	Switch Core de todas las sedes	
	DESASTRES NATURALES	Activación DRP
	INCENDIOS	Activación DRP
	VANDALISMO/SABOTAJE	Activación DRP
OTROS	FALLA EN LA ALIMENTACION ELECTRICA	Activación DRP
	PERDIDA DE LAS COMUNICACIONES (PROVEEDOR DE LINEAS PRIMARIAS Y ENLACES)	Activación DRP

En base al Análisis de impacto de negocio revisado en el capítulo anterior y considerando que primero se deberá tener todo el equipamiento de RED, así como los principales servidores de soporte a los sistemas, se tiene que reponer lo siguiente.

Tabla 21
Prioridad de recuperación 0

SERVIDORES MINIMOS PARA CONTINGENCIA DE MONTERRICO EN SAN ISIDRO	CONTRATO / PROPIO TI / LABORATORIO	Si es contrato: Tiempo de entrega (Hrs)
RHO (Controlador de dominio principal administrativo)	No es necesario	
ADACADMO (Controlador de dominio principal académico)	No es necesario	
FWUPC-Checkpoint (Seguridad Perimetral Monterrico)	No es necesario	
FWACADUPC (Seguridad Perimetral Monterrico Acad.)	No es necesario	
Veritas (Sistema de Backup / Restore) + Robot	Contrato	2

Luego de tener todos los servidores base para la conexión con los sistemas, se deberá realizar la recuperación de prioridad 1, el cuál involucra a los servidores de los sistemas de información.

Tabla 22

Prioridades de Recuperación 1

SERVIDORES MINIMOS PARA CONTINGENCIA DE MONTECRICO EN SAN ISIDRO	CONTRATO / PROPIO TI / LABORATORIO	Si es contrato: Tiempo de entrega (Hrs)
PROD (Base de datos Oracle de Sistema académico)	Propio	
MoodleProd (Aula virtual académica)	Contrato	4
Intranet (Intranet académica)	Contrato	4
SPRING (BBDD y ERP Administrativo UPC)	Contrato	4
SPRINGUPN (BBDD y ERP Administrativo UPN)	Contrato	4
Upmail1 (Correo Administrativo)	Contrato	4
Firewall-IRA (Seguridad entre redes)	No es necesario	
Upmail1a (Correo académico)	Contrato	4

Tabla 23

Prioridades de Recuperación 2

SERVIDORES MINIMOS PARA CONTINGENCIA DE MONTECRICO EN SAN ISIDRO	CONTRATO / PROPIO TI / LABORATORIO	Si es contrato: Tiempo de entrega (Hrs)
DHCP SVR (AD secundario administrativo)	No es necesario	
PortalSql (BBDD del servidor WEB)	Laboratorio	
Aleph (Sistema del Centro de Información)	Laboratorio	
WebUPC (Servidor WWW de UPC)	Laboratorio	
Omega (Servidor de archivos del sistema académico)	Laboratorio	
Beta / SharePoint (Servidor de archivos de administrativos)	Laboratorio	
Beta1A (Servidor de archivos de académicos)	Laboratorio	
Mailing (Servidor de envío de mailing)	Laboratorio	

Tabla 24

Prioridades de Recuperación 3

SEDE	SERVIDORES / SERVICIOS	OBSERVACIONES
MONTECRICO	AdapImo (AD secundario académico)	Atiende el servicio WIFI
	DELFO (Servidor de contenidos)	
	Connect (Servidor de presentaciones)	
	Mailing (Servidor de envío de mailing)	
	DHCPACAD (DHCP académico secundario)	
	Asterisk (Servidor de comunicaciones)	
	DocuShare (Servidor de impresiones)	
	ImpreXerox_1 (Servidor de impresiones)	

CENTRO ALTERNO

De acuerdo a la estrategia y la alternativa de solución seleccionada en el capítulo 3, se procede a definir las condiciones mínimas de infraestructura y equipamiento que deben cumplir el site alterno en caso de ocurrencia de una contingencia. La ubicación física del sitio alterno de recuperación es la siguiente.

Tabla 25

Ubicación de sitio alterno

SITE PRINCIPAL	DIRECCION SITE PRINCIPAL	SITE ALTERNO	DIRECCION SITE ALTERNO
DC Santiago de Surco	Av. Prolongación Otoño 2390	DC San Isidro	Av. Salazar 2450

Las Salas y la infraestructura con la que deberá contar el sitio alterno de acuerdo a la estrategia son las siguientes.

- Sala de Servidores.
 - 01 Rack
 - 01 Switch (24 Puertos de 100/1000 mbps)
 - 01 UPS 500
 - 01 Router (Claro)
- Sala de Comunicaciones.
 - Cisco 5500-G
 - 3Com 4200 G
 - Cisco 2960
 - Cisco 2960
 - Cisco 4100 (12 Aps)
 - 3COM 4228G
 - 3COM 4228G
- Sala de Contingencia.
 - 01 Hub de 8 Puertos
 - 02 Laptop's instaladas con software.
 - 02 Puntos de red disponibles.
- Equipos necesarios para la contingencia

Tabla 26

Equipos necesarios para la contingencia

EQUIPOS NECESARIOS PARA CONTINGENCIA DE MONTECERRICO EN PATCH DE MONTECERRICO QUE SERA ENLACE A SITE ALTERNO (Patch Pab. H ó Patch Pab. J)	CONTRATO / PROPIO TI / LABORATORIO	Si es contrato: Tiempo de entrega (Hrs)
Switch Core Cisco 3750 para red administrativa	Propio	
Switch Core 3Com 5500 para red académica	Propio	
PC DHCP para conexión de estaciones a Site Alterno	Laboratorio	

Tabla 27

Componentes necesarios para la contingencia

COMPONENTES MINIMOS PARA CONTINGENCIA DE MONTECERRICO EN SAN ISIDRO	CONTRATO / PROPIO TI / LABORATORIO	Si es contrato: Tiempo de entrega (Hrs)
Switch adicional de 24 puertos disponible	Propio	
Asegurar 5KVA de energía disponibles en el UPS	Propio	
20 Tomas eléctricas	Propio	
Espacio disponible para 15 servidores	Propio	
20 Cables de red	Propio	
20 cables de poder	Propio	
5 monitores LCD 15"	Propio	
2 estaciones de trabajo	Propio	

PROCEDIMIENTO GENERAL DE RESPUESTA A LA CONTINGENCIA

En caso se produzca un evento que ha interrumpido las operaciones normales de la Sala de Servidores, y el Equipo Coordinador determina que su restablecimiento no puede ser efectuado en un lapso inferior a 48 horas de identificada la contingencia, se procede de la siguiente manera:

- Declaración de la Contingencia
- Activación de los equipos de Trabajo
- Ejecución de Rehabilitación según la fuente de Origen

En el siguiente gráfico se muestra el flujo general de respuesta ante una contingencia, para el caso específico de la universidad, tanto el Centro alternativo de Respaldo y el Ambiente Alternativo para las áreas se encuentran en el Data Center de la sede San Isidro.

Figura 18. Procedimiento de respuesta a la contingencia

ACTIVIDADES DEL PLAN DE RECUPERACION

El propósito es identificar las actividades del plan de recuperación para iniciar y ejecutar los procedimientos previamente definidos. La siguiente tabla es la identificación de los códigos de los equipos o personas responsables de ejecutar diferentes actividades dentro del plan y que estarán asociadas a la tarea como un prefijo de dos caracteres.

Tabla 28
Identificación de prefijos por equipos

Id	Equipo de Recuperación / Persona
EG	Equipo Gerencial
EC	Equipo Coordinador
ES	Equipo de Sistemas
EA	Equipo de Apoyo Administrativo

Id	Equipo de Recuperación / Persona
EU	Equipo de Usuarios
TE	Todos los equipos
XE	Cualquier equipo

La siguiente tabla define la descripción general de cada columna descrita en la tabla de actividades y cómo esta tabla debe ser utilizada.

Tabla 29

Descripción de los campos de las tablas de actividades

Nombre de Columna	Descripción
SEC	Identifica la secuencia de actividades dentro de la recuperación, dos actividades simultáneas tendrán el mismo número de secuencia.
EQ	Identifica el equipo de recuperación encargado de realizar la actividad descrita.
DESCRIPCIÓN	Descripción breve de la actividad a ser ejecutada.
REF	Identifica capítulos o anexos a los cuales se puede recurrir para completar la actividad a ejecutar (Ejemplo: Anexo, capítulo, tabla etc.).

PROCEDIMIENTO DE IDENTIFICACION Y DECLARACION DE CONTINGENCIA

Se determina si una interrupción en la Sala de Servidores puede llegar a tener características de tiempo superior a 48 horas de tal manera que su evaluación lleve a la decisión de declarar oficialmente la contingencia.

Tabla 30
Declaración de contingencia

SEC	EQ	DESCRIPCION	REF
1	XE	Identificar cualquier situación de contingencia en la UPC	
2	XE	Notificar al equipo coordinador la situación identificada.	Anexo A
3	EC	Efectuar una evaluación preliminar de los daños y determinar si el tiempo que estará sin operación la Sala de Servidores es mayor de 48 horas.	
4	EC	Efectuar una evaluación detallada de los daños.	
5	ES	Identificar si la situación obedece a la falla en los equipos de cómputo y determinar si su reparación o reemplazo es mayor a 48 horas de identificada la contingencia. Basado en la revisión de las instalaciones del centro, el funcionamiento de los equipos y el contacto con los proveedores de los mismos.	
6	EC	Comunicar al equipo gerencial la situación presentada y la evaluación realizada.	Anexo A
7	EG	Declarar oficialmente la contingencia y activar el Plan de Recuperación.	

PROCEDIMIENTO DE ACTIVACION DE LOS EQUIPOS DE TRABAJO

Una vez declarada la contingencia, los equipos de trabajo se activarán para iniciar las actividades del plan, de acuerdo a sus responsabilidades. Y se informará a las instancias internas y externas requeridas.

Tabla 31
Activación de equipos de trabajo

SEC	EQ	DESCRIPCION	REF
1	EC	Iniciar contacto con todas las personas involucradas en el desarrollo de las actividades del plan de recuperación.	Anexo A
2	EC	Verificar que todas las personas contactadas estén presentes. Activar los equipos de contingencia, para iniciar operaciones en modalidad de contingencia.	Anexo A
3	EA	Habilitar la contratación de personal temporal y/o reasignación de personal, en caso de que algún equipo de trabajo no esté completo.	
4	EC	Impartir instrucciones adicionales a las especificadas en el plan a los equipos de trabajo indicando responsabilidades y actividades a realizar. Entregar a cada líder de equipo las actividades adicionales a realizar en caso de contingencia.	
5	EG	Notificar la situación a la Dirección (Rectorado) de la universidad.	Anexo A
6	EG	Notificar la situación de Contingencia a las diferentes áreas de la empresa. (Comunicados Internos).	Anexo A
7	EC	Activar procedimientos manuales (DRP).	
8	EG	Enviar comunicado oficial a clientes, proveedores, asesores, medios de comunicación etc. (Comunicados Externos).	Anexo A
9	ES	Ejecutar plan de Rehabilitación según fuentes de origen.	

PROCEDIMIENTO DE REHABILITACION SEGÚN FUENTE DE ORIGEN

Las fuentes de contingencias cubiertas por este plan y las acciones a ejecutar para cada una de ellas se detallan a continuación. Estas fuentes de contingencias se refieren usualmente a diferentes grados dentro de 6 categorías principales: local principal, equipos críticos, comunicaciones de voz y datos, software base y aplicaciones, personal clave y datos. La causa de la pérdida se determina luego del diagnóstico que se realiza, siendo el primer

objetivo del plan de ejecución determinar el grado de pérdida, el impacto en la misión y las técnicas para minimizar este riesgo.

A continuación se presentan los procedimientos de rehabilitación del plan de contingencia:

- CNTG-REH-01 Procedimiento de Respuesta en Caso de Pérdida de Local Principal.
- CNTG-REH-02 Procedimiento de Respuesta en Caso de Pérdida de Equipos Críticos.
- CNTG-REH-03 Procedimiento de Respuesta en Caso de Pérdida de Software Base y Aplicaciones.
- CNTG-REH-04 Procedimiento de Respuesta en Caso de falla de Suministro Eléctrico.

MANTENIMIENTO DEL PLAN DE RECUPERACION

Se define las actividades necesarias para dar mantenimiento al plan de recuperación del área de informática. El mantenimiento del plan es de vital importancia para asegurar la vigencia de lo que se ha recuperado y los procedimientos que rigen la recuperación.

Estos deberán mantener el plan actualizado y sincronizado con los cambios del negocio. Se deberán considerar todos los cambios en las funciones para la inclusión y la actualización del plan de recuperación.

Los cambios están integrados al plan a través del proceso de administración de cambios y problemas y los cambios que se reflejen en la dirección tal y como se identifican en la revisión periódica.

Además de la revisión del plan, se debe hacer un inventario de los datos recuperados y de los materiales que se guardaron fuera de las instalaciones a la misma que se debe hacer una evaluación periódica.

El plan de recuperación puede requerir de actualizaciones en caso de que ocurrieran problemas o cambios en cualquiera de los siguientes aspectos:

- Resultados de prueba de plan de recuperación.
- Aplicaciones críticas o nuevas.
- Mayor complejidad en las aplicaciones.

- Nuevas adquisiciones de equipo.
- Cambios dados por Hardware, Software, Red, Aplicaciones, Datos, Personal y/o Suministros o formas críticas

Figura 19. Diagrama de proceso de control de cambios

BITACORA DE CAMBIOS EN EL PLAN

A continuación se muestra un registro de las actualizaciones de este documento provocadas por el cambio en las consideraciones del plan.

La persona responsable del mantenimiento de dichos documentos deberá colocar la fecha de la actualización y sus iniciales en la columna de revisor cuando se concluyan las actualizaciones.

Tabla 32
Bitácora de cambios

Fecha	Revisor	Tipo de cambio (HW, SW, organización etc.)	Descripción del cambio

5 PRUEBAS, RESULTADOS Y VALIDACION

En este capítulo se describen los resultados y los métodos de validación que se aplicaron al diseño del DRP para la entidad educativa, utilizando para ello los indicadores de logros que se plantearon al inicio del proyecto. A continuación se muestra la tabla de relación de cada logro con el objetivo.

Tabla 33

Relación de cada logro con el objetivo específico

OBJETIVOS ESPECÍFICOS	INDICADORES DE LOGRO	MÉTRICAS
Realizar un Análisis de Riesgos que permita determinar los escenarios de amenazas que podrían afectar al centro de cómputo.	Informe de Análisis de Riesgos Matriz de riesgos.	Escenarios de amenazas críticos o más relevantes. Amenazas de mayor probabilidad de ocurrencia
Desarrollar un Análisis de Impacto al Negocio (BIA), que permita determinar el impacto operacional, económico, que podría tener la universidad como resultado de la ocurrencia de una interrupción o desastre.	Informe de Análisis de Impacto de Negocio (BIA). - Niveles de Servicio - Recursos Críticos - Prioridades de Recuperación - Procesos y Servicios Críticos	Nivel de RPO, RTO y MTPD. Nivel de criticidad de los recursos críticos. Prioridades de recuperación. Nivel de criticidad de procesos y servicios.
Definir las estrategias de recuperación de desastres de TI que permitirán cumplir con los objetivos de recuperación establecidos por el centro de cómputo.	Matriz de estrategias.	Cantidad de Estrategias (N°) - Tiempo - Calidad
Definir las alternativas de solución de recuperación para cada estrategia.	Matriz de Alternativas de Solución.	Cantidad de Alternativas de Solución (N°) - Proveedores

5.1 Resultado de indicador de logro 1

Como resultado de la ejecución del Análisis de Riesgos se determinó la MATRIZ DE RIESGOS el cual identifica el nivel de riesgo en base a la probabilidad por el impacto.

Tabla 34
Matriz de riesgos

Cod.	Clasificación		Valoración del riesgo				
	Factor de Riesgo	Tipo de Evento	Detalle Probabilidad	Nivel de Probabilidad	Detalle del Impacto	Nivel de Impacto	Nivel de Riesgo
R1	4.Eventos Externos	5.Daños a activos materiales	1.2.Bajo	P1	1.2 Bajo	I2	Moderado
R2	4.Eventos Externos	5.Daños a activos materiales	1.1.Muy Bajo	P2	1.5 Muy Alto	I5	Extremo
R3	3.Tecnología	6.Interrupción del Negocio / fallo en el sistema	1.3.Medio	P3	1.4 Alto	I4	Extremo
R4	2.Personas	7.Ejecución entrega y gestión de procesos	1.3.Medio	P3	1.5 Muy Alto	I5	Extremo
R5	4.Eventos Externos	6.Interrupción del Negocio / fallo en el sistema	1.3.Medio	P3	1.5 Muy Alto	I5	Extremo
R6	4.Eventos Externos	6.Interrupción del Negocio / fallo en el sistema	1.1.Muy Bajo	P1	1.5 Muy Alto	I5	Extremo

La ubicación de los riesgos en el mapa es el siguiente.

Tabla 35
Mapa de riesgo

PROBABILIDAD	P.5	MODERADO	EXTREMO	EXTREMO	EXTREMO	EXTREMO
	P.4	MODERADO	ALTO	EXTREMO	EXTREMO	EXTREMO
	P.3	MODERADO	ALTO	EXTREMO	EXTREMO (R4)	EXTREMO (R5, R3)
	P.2	BAJO	MODERADO (R1)	ALTO	EXTREMO	EXTREMO (R2)
	P.1	BAJO	BAJO	MODERADO	ALTO	EXTREMO (R6)
		I.1	I.2	I.3	I.4	I.5
		IMPACTO				

Se tiene que los escenarios de amenazas identificados como R2, R3, R4, R5, R6 tienen riesgo EXTREMO, mientras que el escenario de amenaza R1 tiene un nivel de riesgo MODERADO.

5.2 Resultado de indicador de logro 2

Como resultado de la ejecución del Análisis de Impacto de Negocio, se tiene la relación de subprocesos con la clasificación de la criticidad. Los subprocesos evaluados fueron los siguientes.

Tabla 36
Sub procesos con criticidad Alta

Sub Procesos	Prioridad de Recuperación	Máximo Tiempo Tolerable de Interrupción (MTPD)	Clasificación del Subproceso	RTO Estimado
Evaluación / incorporación	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Telemarketing	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Gestión de multicanales	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Facturación	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Cobranza	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Matricula	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Crm	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Mantenimiento de infraestructura	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Cursos blended	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Cursos full	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 horas
Soporte de aplicaciones académicas	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 Horas
Soporte de aplicaciones financieras	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 Horas
Servicios de ti (soporte)	Nivel-2	<= 8 Horas	Criticidad Alta	< 4 Horas

Tabla 37
Sub procesos con criticidad media

Sub Procesos	Prioridad de Recuperación	Máximo Tiempo Tolerable de Interrupción (MTPD)	Clasificación del Subproceso	RTO Estimado
Prospección	Nivel-6	<= 14 Días	Criticidad Media	< 10 Días
Seguimiento – Cierre	Nivel-6	<= 14 Días	Criticidad Media	< 10 Días
Definición de Curricula	Nivel-5	<= 7 Días	Criticidad Media	< 5 Días
Programación de Horarios	Nivel-5	<= 7 Días	Criticidad Media	< 5 Días
Cierre del ciclo anterior	Nivel-5	<= 7 Días	Criticidad Media	< 5 Días
Nuevos ingresos - Admisión	Nivel-4	<= 48 Horas	Criticidad Media	< 24 horas
Becas y Créditos	Nivel-6	<= 14 Días	Criticidad Media	< 10 Días
Monitoreo y cumplimiento de políticas	Nivel-6	<= 14 Días	Criticidad Media	< 10 Días
Administración de accesos	Nivel-4	<= 48 Horas	Criticidad Media	< 24 horas
Gestión de Incidentes de Seguridad de Información	Nivel-4	<= 48 Horas	Criticidad Media	< 24 horas
Seguridad Física - Control Patrimonial	Nivel-5	<= 7 Días	Criticidad Media	< 72 horas
Sistema de Salud en el Trabajo	Nivel-6	<= 14 Días	Criticidad Media	< 07 Días

Tabla 38
Sub procesos con criticidad baja

Sub Procesos	Prioridad de Recuperación	Máximo Tiempo Tolerable de Interrupción (MTPD)	Clasificación del Subproceso	RTO Estimado
Políticas – reglamento	Nivel-7	<= 30 Días	Criticidad Baja	< 15 Días
Trámites	Nivel-7	<= 30 Días	Criticidad Baja	< 15 Días
BI	Nivel-7	<= 30 Días	Criticidad Baja	< 15 Días
Carga de información	Nivel-8	>30 Días	Criticidad Baja	<20 Días
Biblioteca Aleph	Nivel-7	<= 30 Días	Criticidad Baja	< 15 Días
Aseguramiento y control de calidad	Nivel-7	<= 30 Días	Criticidad Baja	< 15 Días

De los subprocesos analizados se obtiene como resultado que el 42% se ha clasificado con nivel de criticidad ALTO por los propietarios del proceso, el 39% con criticidad MEDIA y el 19% con criticidad BAJA.

Figura 20. Clasificación de los Sub-procesos

5.3 Resultado de indicador de logro 3

Como resultado de logro para el tercer objetivo específico, se evaluó la matriz de estrategias de recuperación, sobre la cual se identificaron 4 posibles clases.

Tabla 39
Matriz de estrategias

TIPO DE SITIO ALTERNO	COSTO	EQUIPAMIENTO DE HARDWARE	COMUNICACIÓN	TIEMPO CONFIGURACIÓN	SITIO
COLD	Bajo	Ninguno	Ninguno	Largo Entre 24 y 72 horas	Centro de Computo Alterno
WARM	Medio	Parcial	Parcial / Completo	Medio Entre 8 y 24 horas	Centro de Computo Alterno / Nube
HOT	Alto	Completo	Completo	Corto Entre 4 y 8 horas	Centro de Computo alternativo / Nube
MIRROR	Muy Alto	Completo	Completo	Ninguno 0 horas	Centro de Computo Alterno / Cloud

De acuerdo a la matriz de estrategias presentadas en el cuadro anterior y evaluando que se necesita un equipamiento completo de Hardware, el sistema de comunicación debe estar completo y disponible en todo momento, considerando que el tiempo de configuración será muy corto y que se requiere de un centro de cómputo alternativo de manera física o en la nube, se ha decidido optar por la estrategia de HOT SITE para la recuperación del centro de cómputo de la universidad.

5.4 Resultado de indicador de logro 4

Luego de haber seleccionar la estrategia, se tiene las siguientes alternativas de solución, que se detallan en la matriz de alternativas de solución.

Tabla 40
Matriz de alternativas de solución por estrategias

Tipo	Alternativas de Solución	Tipo de Alternativas	Implementador
------	--------------------------	----------------------	---------------

HOT SITE	Local propio	Implementación de site alternativo con infraestructura propia	Personal interno en San Isidro. Personal de interno en Sede Villa.
	Hosting	DC externo con infraestructura equipada en local de proveedor	<u>Proveedores</u> ITG SOLUTIONS. CLARO. NET SECURE. IBM LEVEL3
	Cloud	DC en nube	<u>Proveedores</u> AZURE AMAZON IBM
MIRROR SITE	Local	Replicación directa hacia el data center externo.	<u>Proveedores</u> ITG SOLUTIONS. CLARO. NET SECURE. IBM LEVEL3
	Cloud	Replicación a data center en nube	<u>Proveedores</u> AZURE AMAZON IBM VMWARE (DRaaS)

La organización cuenta con un centro de cómputo alternativo, así como infraestructura propia para soportar los procesos críticos de negocio; es por ello, de las alternativas de solución que se plantea se elige el Local Propio, con esta alternativa la universidad ahorrará costos al no tener que invertir en equipamiento.

La sede seleccionada para la implantación del DRP será la sede San Isidro. En un futuro no muy lejano es probable que se pueda migrar al tipo de configuración MIRROR SITE.

5.5 Plan de Pruebas de DRP

Objetivos del Plan de Pruebas.

Practicar los procedimientos ante un incidente o desastre. Identificar áreas que necesitan mejorar. Permitir al DRP permanecer activo, actualizado, entendible y usable. Demostrar la habilidad de recuperación.

Alcance de las pruebas

Las pruebas deben ejecutarse durante un tiempo en el que las afectaciones de la operación normal sean mínimas y debe comprender elementos críticos y simular condiciones de proceso, aunque se realicen fuera del horario laboral de la universidad. Las pruebas deben incluir las siguientes tareas.

- Verificar la totalidad y precisión del plan.
- Evaluar el desempeño del personal involucrado.
- Evaluar la coordinación entre los miembros de los comités, proveedores y otros terceros.
- Identificar la capacidad de recuperar registros e información vital.
- Medir el desempeño de los sistemas operativos y computaciones.

Durante esta etapa se debe establecer un programa de pruebas con escenarios simulados, planeados en el tiempo, teniendo en cuenta los requerimientos de cada prueba y con una revisión exhaustiva de los resultados de las mismas, para generar mejoras a los planes.

Tabla 41
Escenario de Plan de Pruebas

	Servicio Afectado	Consecuencia	Afectado por
1	Centro de Cómputo Principal	No disponibilidad del centro de cómputo	Atentado, incendio, inundación, daño sistema aire acondicionado, daño suministro eléctrico.
2	Infraestructura de comunicaciones	No disponibilidad de los servicios de comunicaciones por fallas.	Switch core, fibras ópticas, enlaces de comunicación con ISP, firewall.
3	Infraestructura de Servidores	No disponibilidad de la infraestructura por fallas	Servidores críticos de la universidad.
4	Infraestructura de Bases de datos, Almacenamiento y Respaldo	No disponibilidad de datos e información.	Corrupción de la base de datos, borrado o pérdida de datos, falla total en almacenamiento, falla total en la SAN, falla total en servidor de respaldo.

Actividades de notificación, evaluación y activación del DRP.

Los usuarios deben reportar el incidente a la mesa de ayuda cuando:

- No se pueden utilizar los sistemas de información de la universidad.
- No hay red de comunicaciones.
- No hay servicio de correo electrónico.
- No hay acceso a los archivos electrónicos centralizados.
- Cualquier otro evento de tecnología que afecte la prestación del servicio.

El personal administrativo (vigilancia, servicios generales) deben reportar el incidente a Mesa de Ayuda o Líder de Centro de Cómputo cuando:

- Suena la alarma del centro de cómputo.
- Hay inundación en cualquier piso.
- Hay un amago de incendio en el piso donde se encuentre ubicado el centro de cómputo.
- Cualquier otro evento que afecte o pueda afectar el centro de cómputo.

La mesa de ayuda debe atender el incidente de acuerdo a lo establecido en sus procedimientos si:

- El incidente afecta la disponibilidad de los sistemas, a nivel general.
- El incidente afecta la disponibilidad de la red de comunicaciones a nivel general.
- Ningún usuario tiene acceso al correo electrónico.
- Ningún usuario puede acceder a sus archivos electrónicos centralizados.

En cualquiera de los casos, debe escalarlo a los funcionarios responsables. El profesional especializado de la plataforma afectada, debe realizar un diagnóstico sobre el incidente presentado, teniendo en cuenta:

- Naturaleza e impacto del incidente.
- Estrategias definidas en el DRP aplicables u otras soluciones potenciales.
- Tiempo estimado de solución del incidente.

Finalmente, comunicarse con el Gerente de TI para informar los resultados del diagnóstico.

El Gerente de TI define si se activa o no el centro de cómputo alterno, teniendo en cuenta los siguientes aspectos:

- Si el evento afectó considerablemente el Centro de Cómputo Principal.
- Si la solución en sitio dura más de 24 horas.

En caso de que se active, se debe comunicar la activación al personal del centro de cómputo de contingencia, en la sede San Isidro, teniendo en cuenta:

- Fecha y hora a partir de la cual se da inicio a la activación.
- Gerente de operaciones de la sede que estaría en el proceso de activación, para que se tramiten los permisos de acceso correspondientes.

El Líder de Infraestructura, coordina la ejecución de las actividades para recuperar la plataforma en el Centro de Cómputo Alterno, teniendo en cuenta:

- Enrutamiento y activación de las comunicaciones hacia el Centro de Cómputo Alterno.
- Detención de la replicación de datos.
- Verificación de la disponibilidad de información en el Centro de Cómputo Alterno.
- Activación servicio de controladores de dominio y sistema operativo en servidores.
- Activación servicio de bases de datos y aplicaciones.

El Líder de infraestructura, verifica la disponibilidad de la plataforma desde el Centro de Cómputo Alterno, teniendo en cuenta:

- Acceder a los sistemas de información.
- Realizar pruebas sobre los sistemas de información.

El Gerente de TI. Define si comunica o no el incidente a la Alta Dirección, caso en el cuál se realizarían las actividades de manejo de crisis.

El líder responsable de la plataforma afectada, activa las estrategias de contingencia locales, teniendo en cuenta los siguientes aspectos:

Si es un evento que afectó las comunicaciones.

- Configurar el switch de contingencia, en caso de falla en el switch core.
- Contactar al proveedor de comunicaciones, en caso de falla en el router de enlaces con ISP.
- Enrutar el tráfico por los demás switch que componen el stack, en caso de una falla de la fibra óptica de uno de ellos.

- Utilizar el switch de piso como contingencia ante falla de un switch de piso en un centro de cableado.
- Configurar el firewall de contingencia, en caso de falla del equipo principal.
- Si es un evento que afectó la infraestructura de servidores.
- Configurar el servidor de contingencia en el BladeServer utilizando la plantilla predefinida en la plataforma VMware Center, para cada tipo de sistema.
- Activar los servidores de contingencia.
- Si es un evento que afectó Infraestructura de Base de Datos Almacenamiento y Respaldo.
- Recuperación de información y bases de datos desde los respaldos, en caso de corrupción de la base de datos, y borrado o pérdida de datos.
- Utilizar los discos de contingencia ante una falla en la SAN.
- Configurar el servidor de contingencia como servidor de respaldo, en caso de falla del principal.

El líder responsable de la Plataforma afectada solicita la contratación urgente de los servicios y equipos necesarios para la solucionar el incidente.

El Gerente de TI realiza la gestión para la contratación o compra de servicios y/o equipos, de ser necesarios, para solucionar el incidente.

El líder responsable de la plataforma afectada coordina la solución con el proveedor contratado.

El Gerente de TI comunica la solución del incidente a la entidad.

El Gerente de TI, en conjunto con los profesionales especializados, define la estrategia de retorno a la normalidad, teniendo en cuenta:

- Fecha de retorno a operación normal.
- Consideraciones especiales a aplicar en el proceso de retorno.
- Consideraciones especiales con respecto a la recuperación de la información y mantener la integridad de los datos, cuando aplique.
- Sincronización entre los centros de cómputo, cuando se operó en el centro de cómputo alterno, según sea el caso.

Todos los miembros de los equipos que participaron en la atención del incidente, documentan el incidente e identifican oportunidades de mejora para fortalecer el DRP.

Se realiza el cierre del incidente, interrupción mayor o evento de contingencia, y se continúa con la ejecución del procedimiento de acciones preventivas y correctivas.

PLAN DE PRUEBAS - 2019		2019											
	Responsable	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SET	OCT	NOV	DIC
Pruebas de Continuidad Tecnológica													
Pruebas Unitarias (Disponibilidad y Conectividad)	Sistemas												
Prueba de Procesamiento en diferente Sede (Sede Alternativa)	Sistemas												
Simulacro: Interrupción total del Centro de Computo Principal	Sistemas												
Planes de Emergencia													
Plan de Emergencia en Sedes	Seguridad Física												
Plan de Emergencia en Sede Monterrico	Seguridad Física												
Plan de Emergencia en Chorrillos	Seguridad Física												
Gestión de Crisis													
Ejercicio de Respuesta: Falla total del Centro de Cómputo por dos días	Sistemas												
Simulacro: Interrupción total del Centro de Computo Principal	Sistemas												
Pruebas de Escritorio													
Destrucción de Sede Monterrico	Sistemas												
Falla Total de Sistemas	Sistemas												
Indisponibilidad de Acceso a la Sede Monterrico	Sistemas + Seg Física												
Indisponibilidad de Personal	RRHH												
Indisponibilidad de Proveedores	Sistemas + Seg Física												
Terremoto en Lima	Sistemas + Seg Física												
Pruebas en Vivo													
Plan de Continuidad de Sede Alternativa	Sistemas												
Indisponibilidad de Acceso a la Sede Monterrico	Sistemas												
Destrucción de la Sede Monterrico	Sistemas												
Falla Total de Sistemas	Sistemas												
Pruebas de Sede Alternativa													
Indisponibilidad de Acceso a la Sede Monterrico	Continuidad del Negocio												

Figura 21. Plan de pruebas 2019

5.6 Validación de ejecución del Plan

La ejecución de este test o prueba de DRP se realizó físicamente en la sede San Isidro y se utilizó como infraestructura de servidores dos equipos HP ProLiant BL460c Gen9 y un HP ProLiant BL460c G7 en los que se implementaron servidores virtuales con VMWare y el TAPE server para la conexión con la consola de Veeam backup.

La tarea inicial fue la revisión de la infraestructura de hardware para poder implementar los servidores virtuales de la prueba de DRP. La cantidad de infraestructura de hardware usada para la implementación de este ambiente de prueba de DRP fueron las siguientes:

- 1 Blade ProLiant BL460c Gen9, las características de hardware de este equipo son:
 - 32 Procesadores de 2.60 GHz
 - 256 GB RAM
 - IP: 10.10.85.XX
 - HOSTNAME: SVRESXIDRP01
 - BAHÍA 01

- 1 Blade ProLiant BL460c Gen9, las características de hardware de este equipo son:
 - 24 Procesadores de 2.60 GHz
 - 96 GB RAM
 - IP: 10.10.85.XX
 - HOSTNAME: SVRESXIDRP02
 - BAHÍA 02

10.10.85

Hypervisor: VMware ESX, 6.7.0, 10302608

Modelo: HP ProLiant BL460c Gen9

Tipo de procesador: Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz

Procesadores lógicos: 24

NIC: 8

Máquinas virtuales: 3

Condición: Conectado

Tiempo de actividad: 3 días

Hewlett Packard Enterprise

CPU: LIBRE 29.37 GHz

USADO: 347.00 MHz CAPACIDAD: 28.76 GHz

MEMORIA: LIBRE 87.11 GB

USADO: 8.75 GB CAPACIDAD: 95.87 GB

ALMACENAMIENTO: LIBRE 10.03 TB

USADO: 6.32 TB CAPACIDAD: 22.35 TB

C7000_ENCL_2_MO

Front View

Device Bay 2

ProLiant BL460c Gen9

Name: SVRESXIDRP02

iLO IPv4 Address: 10.10.85

Information

Server Name: SVRESXIDRP02

Product Name: ProLiant BL460c Gen9

UUID: 30373237-3132-4D32-3234-353130324352

Server Serial Number: 2M245102CR

Product ID: 727021-B21

System ROM: I36 v2.56 (01/22/2018)

System ROM Date: 01/22/2018

Backup System ROM: I36 v1.21 (11/03/2014)

Integrated Remote Console: [.NET](#) [Java Web Start](#) [Java Applet](#)

License Type: iLO Standard Blade Edition

iLO Firmware Version: 2.55 Aug 16 2017

IP Address: 10.10.85

Link-Local IPv6 Address: FE80::FE15:B4FF:FE8E:B388

iLO Hostname: ILO2M245102CR.upc.edu.pe

Server NIC Information		Device ID
FLB Adapter 1: HP FlexFabric 10Gb 2-port 536FLB Adapter		
Ethernet FlexNIC (NIC 0) LOM1:1-a	6C:C2:17:39:1F:E0	
Ethernet FlexNIC (NIC 2) LOM1:1-b	6C:C2:17:39:1F:E1	
Ethernet FlexNIC LOM1:1-c	6C:C2:17:39:1F:E2	
Ethernet FlexNIC LOM1:1-d	6C:C2:17:39:1F:E3	
Ethernet FlexNIC (NIC 1) LOM1:2-a	6C:C2:17:39:1F:E8	
Ethernet FlexNIC (NIC 3) LOM1:2-b	6C:C2:17:39:1F:E9	
Ethernet FlexNIC LOM1:2-c	6C:C2:17:39:1F:EA	
Ethernet FlexNIC LOM1:2-d	6C:C2:17:39:1F:EB	
Management Processor		iLO FC:15:B4:8E:B3:88

Mezzanine Card Information			
Mezzanine Slot	Mezzanine Device	Mezzanine Device Port	Device ID
2	HP LPe1605 16Gb FC HBA for BladeSystem c-Class		
		Port 1	10:00:28:80:23:de:dc:1a
		Port 2	10:00:28:80:23:de:dc:1b

CPU and Memory Information	
CPU 1	Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 Cores)
CPU 2	Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz (6 Cores)
Memory	98304 MB

- 1 HP ProLiant BL460c G7, las características de hardware de este equipo son:
 - 12 Procesadores de 2.67 GHz
 - 16GB RAM
 - Bahía 09 (SVRDRPVVEAMMO)

C7000_ENCL_2_MO

Front View

Device Bay 9

ProLiant BL460c G7

Name: SVRDRPVVEAMMO

iLO IPv4 Address: 10.10.85 [REDACTED]

Information

Server Name	SVRDRPVVEAMMO
Product Name	ProLiant BL460c G7
UUID	37333036-3831-5355-4531-323642563253
Server Serial Number	USE126BV2S
Product ID	603718-B21
System ROM	I27 08/16/2015
Backup System ROM	01/29/2011
Integrated Remote Console	.NET Java Web Start Java Applet
License Type	iLO 3 Standard Blade Edition
iLO Firmware Version	1.88 Jul 13 2016
IP Address	10.10.85 [REDACTED]
Link-Local IPv6 Address	FE80::9A4B:E1FF:FE7B:8E8F
iLO Hostname	ILOUSE126BV2S.upc.edu.pe

Server NIC Information		Device ID
FlexFabric Embedded Ethernet		
Ethernet FlexNIC (NIC 1) LOM:1-a	78:E3:B5:17:00:D8	
Ethernet FlexNIC (NIC 3) LOM:1-b	78:E3:B5:17:00:D9	
Ethernet FlexNIC (NIC 5) LOM:1-c	78:E3:B5:17:00:DA	
Ethernet FlexNIC (NIC 7) LOM:1-d	78:E3:B5:17:00:DB	
Ethernet FlexNIC (NIC 2) LOM:2-a	78:E3:B5:17:00:DC	
Ethernet FlexNIC (NIC 4) LOM:2-b	78:E3:B5:17:00:DD	
Ethernet FlexNIC (NIC 6) LOM:2-c	78:E3:B5:17:00:DE	
Ethernet FlexNIC (NIC 8) LOM:2-d	78:E3:B5:17:00:DF	
Management Processor		iLO 98:4B:E1:7B:8E:8F

Mezzanine Card Information			
Mezzanine Slot	Mezzanine Device	Mezzanine Device Port	Device ID
2	Emulex LPe1205-HP 8Gb FC HBA for HP BladeSystem c-Class		
		Port 1	10:00:00:00:c9:ba:a4:10
		Port 2	10:00:00:00:c9:ba:a4:11

CPU and Memory Information	
CPU 1	Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (6 Cores)
CPU 2	Intel(R) Xeon(R) CPU X5650 @ 2.67GHz (6 Cores)
Memory	16384 MB

- 3. Tb en espacio de disco en el 3PAR 7.200
 - Reservados para las máquinas virtuales ADMO0102, INTRANET02, SPRING02, DESKTOP_PC02 y SVRPRDVEEAMC02.

Name	Domain	Set	State	Type	Provisioning	RAID	Virtual Size (GB)	Reserved User Size (GB)	Reserved User Size (% Virtual)	Reserved Copy Size (GB)	Reserved Copy Size (% Virtual)	Exported To
DRP_VOLUME_01	--	--	Normal	Base	Thin	RAID 5	3,072.000	1,035.375	33%	--	--	SVRDRPROD1, SVRDRPROD2

DRP_VOLUME_01		Acciones
Introducción	Resumen	Supervisar
<p>DRP_VOLUME_01</p> <p>Tipo: VMFS 5</p> <p>URL: ds:///vmfs/volumes/5bf5c30b-c867120e-ee2f-5cb001d9b0e0/</p>		<p>ALMACENAMIENTO LIBRE: 449.54 GB</p> <p>USADO: 2.67 TB CAPACIDAD: 3.00 TB</p> <p>Actualizar</p>
Configurar		Permisos
Archivos		Hosts
Máquinas virtuales		

- 7.13 Tb en espacio de disco en el 3PAR
 - Reservados para los servidores físicos SVRPROD1 y SVRPROD2

Name	Domain	Host Ports	Storage System Ports	Node ID(s)	Persona	Volumes Exported	Total Reserved Size (GiB)	Total Exported Size (GiB)
SVRDRPROD1	--	2	4	0,1	15 - WindowsServer	15	3,405.000	3,405.000
SVRDRPROD2	--	2	4	0,1	15 - WindowsServer	16	3,905.000	3,905.000

Name	Set	State	Type	Provisioning	RAID	Virtual Size (GB)	Reserved User Size (GB)	Reserved User Size (% Virtual)	Reserved Copy Size (GB)	Reserved Copy Size (% Virtual)	Exported To
OCR_DRP	--	● Normal	Base	Full	RAID 5	1.000	1.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
OCR2_DRP	--	● Normal	Base	Full	RAID 5	1.000	1.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
VOTINDISK1_DRP	--	● Normal	Base	Full	RAID 5	1.000	1.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
VOTINDISK2_DRP	--	● Normal	Base	Full	RAID 5	1.000	1.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
ASMDATA2_DRP	--	● Normal	Base	Full	RAID 5	400.000	400.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
ASMDATA5_DRP	--	● Normal	Base	Full	RAID 5	400.000	400.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
ASMPRA2_DRP	--	● Normal	Base	Full	RAID 5	400.000	400.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
ASMPRED02_DRP	--	● Normal	Base	Full	RAID 5	100.000	100.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
ASMDATA6_DRP	--	● Normal	Base	Full	RAID 5	400.000	400.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
VOTINDISK3_DRP	--	● Normal	Base	Full	RAID 5	1.000	1.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
ASMPRED01_DRP	--	● Normal	Base	Full	RAID 5	100.000	100.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
ASMPRA1_DRP	--	● Normal	Base	Full	RAID 5	400.000	400.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
ASMDATA1_DRP	--	● Normal	Base	Full	RAID 5	400.000	400.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
ASMDATA3_DRP	--	● Normal	Base	Full	RAID 5	400.000	400.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
ASMDATA4_DRP	--	● Normal	Base	Full	RAID 5	400.000	400.000	100%	--	--	SVDRPPROD1, SVDRPPROD2
Backupdpprod	--	● Normal	Base	Full	RAID 5	500.000	500.000	100%	--	--	SVDRPPROD2

Todas las tareas indicadas no deben de constar como tiempos de recuperación de los servidores teniendo en cuenta que deberíamos reservar infraestructura de servidores similar para un caso real de Disaster Recovery.

A continuación, se muestran las pantallas de la instalación de los ambientes de pruebas para la posterior restauración de la información.

Características de los servidores virtuales para el sistema.

Se trabajó con servidores virtuales:

Nodo 01, las características de hardware de este equipo son:

24 Procesadores de 2.60 GHz

64GB RAM

Ubicación: SVRESXIDRP0102

Hostname: SVRPROD102

Nodo 02, las características de hardware de este equipo son:

24 Procesadores de 2.60 GHz

64GB RAM

Ubicación: SVRESXIDRP0202

Hostname: SVRPROD202

Servidores virtuales instalados en el servidor Blade BL460c G7:

La distribución de los servidores virtuales en los servidores Blades fue:

En el SVRESXIDRP01 (HP ProLiant BL460c Gen9) se instalaron los servidores SPRING02, SVRDRPVCENTER02, SVRDRPVEEAMC02, SVRPRDINTMO0102 y SVRPROD02.

Nombre	Estado	Condición	Espacio aprovisionado	Espacio utilizado	CPU de host	Memoria de host
SVRPROD	Encendido	Normal	3,58 TB	3,58 TB	181 MHz	64.018 MB
SVRPRDINTMO01	Encendido	Normal	484,11 GB	484,11 GB	233 MHz	24.679 MB
SVRDRPVEEAMC	Encendido	Normal	108,12 GB	108,12 GB	1.012 MHz	8.256 MB
SVRDRPVCENTER	Encendido	Normal	108,19 GB	108,19 GB	2.518 MHz	8.259 MB
SPRING	Encendido	Normal	1,3 TB	1,3 TB	207 MHz	36.289 MB

En el SVRESXIDRP02 (HP ProLiant BL460c Gen9) se instalaron los servidores ADMO01, DESKTOP_PC y SVRPROD2.

Nombre	Estado	Condición	Espacio aprovisionado	Espacio utilizado	CPU de host	Memoria de host
SVRPROD2	Encendido	Normal	4,07 TB	4,07 TB	838 MHz	59.780 MB
SVRDRPADMO01	Encendido	Normal	308,12 GB	8,36 GB	0 MHz	3.867 MB
DESKTOP_PC	Encendido	Normal	103,11 GB	103,11 GB	0 MHz	1.824 MB
ADMO01	Encendido	Normal	324,11 GB	206,63 GB	743 MHz	24.700 MB

Sistemas operativos levantados de ADMO01, SPRING e INTRANET:

ADMO01

ADMO01

Acciones ▼

Introducción Resumen Supervisor Configurar Permisos Instantáneas Almacenes de datos Redes

Encendido

ADMO01

Sistema operativo invitado: Microsoft Windows Server 2008 R2 (64-bit)
Compatibilidad: ESX/ESXi 4.0 y posterior (máquina virtual versión 7)
VMware Tools: En ejecución, versión: 10279 (Actualización disponible)
[Más información...](#)
Nombre DNS: ADMO01.UPC.EDU.PE
Direcciones IP: 10.10.85.20
Host: 10.10.85.16

USO DE CPU
671,00 MHz

USO DE MEMORIA
1,44 GB

USO DE ALMACENAMIENTO
206,63 GB

The screenshot shows the Windows DNS Manager interface. On the left pane, the tree view is expanded to show the hierarchy under 'DNS' > 'ADMO01'. The 'Forward Lookup Zones' are listed, including '_msdcs.upc.edu.pe', 'mailing.upc.edu.pe', 'fondocedior.upc.edu.pe', 'low.corp', and 'upc.edu.pe'. Under 'upc.edu.pe', several sub-zones are visible, such as '_domainkey', '_sites', '_tcp', '_tls', '_udp', 'admission', 'campusinstitucional', 'DomainDnsZones', 'em', 'encuesta', 'epe', 'esproxy', 'esproxysdo', 'ForestDnsZones', 'innovacioneducativa', 'is', 'noticias', 'postgrado', 'puntoseguido', 'SVRDESAAPPNO02', 'tienda', 'vida', and 'upc.pe'. Below these are 'Reverse Lookup Zones' and 'Conditional Forwarders'.

The right pane displays a table of DNS records for the selected zone. The table has three columns: Name, Type, and Data.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[17051561], admo01.upc.edu.pe., admin.upc.edu.pe.
(same as parent folder)	Name Server (NS)	admo04.upc.edu.pe.
(same as parent folder)	Name Server (NS)	admo01.upc.edu.pe.
(same as parent folder)	Name Server (NS)	admo03.upc.edu.pe.
(same as parent folder)	Name Server (NS)	adct01.upc.edu.pe.
(same as parent folder)	Name Server (NS)	admo02.upc.edu.pe.
(same as parent folder)	Name Server (NS)	adct02.upc.edu.pe.
(same as parent folder)	Name Server (NS)	ads04.upc.edu.pe.
(same as parent folder)	Name Server (NS)	adv01.upc.edu.pe.
(same as parent folder)	Name Server (NS)	ads01.upc.edu.pe.
(same as parent folder)	Name Server (NS)	ads03.upc.edu.pe.
(same as parent folder)	Name Server (NS)	adv02.upc.edu.pe.
(same as parent folder)	Name Server (NS)	ads02.upc.edu.pe.
(same as parent folder)	Name Server (NS)	adsm01.upc.edu.pe.
(same as parent folder)	Host (A)	10.142.3.11
(same as parent folder)	Host (A)	10.142.3.8
(same as parent folder)	Host (A)	10.21.0.3
(same as parent folder)	Host (A)	10.11.0.14
(same as parent folder)	Host (A)	10.142.224.3
(same as parent folder)	Host (A)	10.142.97.11
(same as parent folder)	Host (A)	10.20.0.44
(same as parent folder)	Host (A)	10.142.224.10
(same as parent folder)	Host (A)	10.21.0.45
(same as parent folder)	Host (A)	10.10.1.10
(same as parent folder)	Host (A)	10.10.85.20
(same as parent folder)	Host (A)	10.11.0.22
(same as parent folder)	Host (A)	10.20.0.45
(same as parent folder)	Mail Exchanger (MX)	[20] svmail01v.upc.edu.pe.
(same as parent folder)	Mail Exchanger (MX)	[10] svmail01m.upc.edu.pe.
_domainkey		
_sites

INTRANET

Servidores de BD – Oracle

SVRPROD1

Este servidor virtual se encuentra alojado el servidor de BD para el Nodo 1.

SVRPROD2

Este servidor virtual se encuentra alojado el servidor de BD para el Nodo 2.

Catalogado de cintas:

El catalogado de cintas, son procesos u operaciones en la cual las cintas son originalmente respaldadas en el Veeam Backup y son reconocidas en otro (para este ejercicio se creó un Veeam Backup and Replication 9.5 para el DRP), demoran en promedio de 15 a 30 minutos por cada cinta.

La relación de cintas que tuvieron que importarse o catalogarse para este trabajo de DRP fueron 4 cintas:

NAME	DESCRPCIÓN	MENSUAL
UPC024L7	JOB FISICOS (MO & SI)	Octubre
UPC044L7	JOB VIRTUALES (MO)	Octubre
UPC020L7	JOB VIRTUALES (MO)	Octubre
UPC019L7	JOB VIRTUALES (MO)	Octubre

A continuación, se copian muestras de los logs de catalogado de cintas, en donde se puede ver el tiempo que demora estas operaciones:

Se puede apreciar que la catalogación de cintas con la solución de Veeam dura entre 15 minutos hasta 30 minutos dependiendo de la cantidad de información respaldada.

TIEMPOS DE RESTAURACIÓN

ACCIÓN	Tiempos	JOB	SERVIDOR
Desencriptar	5 minutos	Backup_Job_SERVERS_1_MO	SVRPRDINTMO01
Importar	20 minutos		
Restauración	35 minutos		
Desencriptar	5 minutos	Backup_Job_SERVERS_2_MO	ADMO01
Importar	6 minutos		
Restauración	25 minutos		
Desencriptar	5 minutos	Backup_Job_SERVERS_3_MO	SPRING
Importar	15 minutos		
Restauración	56 minutos		

CONCLUSIONES

En base a los resultados obtenidos se concluye lo siguiente.

- En muchos casos, la importancia que tiene contar con un DRP consistente, eficaz y actualizado que permita minimizar el tiempo de interrupción de los servicios de IT en una compañía se hace evidente cuando se producen situaciones de desastres que ponen en riesgo los activos informáticos generando consecuencias desfavorables para la organización.
- La planificación es crítica a la hora de evitar y enfrentar los desastres informáticos. Para ello, es necesario que las organizaciones tengan en cuenta en el día a día los diferentes procesos para la continuidad de las operaciones, como almacenamiento, protección de datos, recuperación efectiva de información, entre otros, que sean fuertes, pero a la vez fáciles de incorporar e implementar, asegurando así la permanencia, integridad y disponibilidad de la información.
- Según los niveles de criticidad desde la óptica de la continuidad operacional y mediante una valoración, algunos procesos correspondientes a las diferentes áreas, no han sido clasificados con Criticidad Alta para la entidad educativa; sin embargo, se debe tener en cuenta que este resultado podría variar por un factor de dependencia con otros procesos de negocio.
- Se ha determinado el MTPD (Máximo Tiempo Tolerable de Interrupción) para cada subproceso, el cual indica el tiempo en que el proceso puede estar sin prestar servicio y sin causar un impacto negativo significativo en el negocio.

Se ha obtenido información de las dependencias tecnológicas de cada uno de los subprocesos, las cuales fueron analizadas para el establecimiento de las estrategias de recuperación.

RECOMENDACIONES PARA TRABAJOS FUTUROS

El presente proyecto de fin de carrera, ofrece una serie de oportunidades para posibles trabajos futuros, entre los que se encuentra:

- Ampliación de escenarios para el desarrollo del DRP, como por ejemplo otros tipos de desastres naturales, incendios, manifestaciones o huelgas, que se puedan presentar en el país.
- Debido a que los planes sólo funcionan cuando se prueban y validan, es necesario poner en marcha estrategias y escenarios de prueba (de peligro, posibles ataques informáticos, incendios, terremotos, entre otros) para determinar las áreas en las que la organización necesita realizar esfuerzos adicionales para responder a sus propios retos y a las amenazas emergentes.
- Cobertura de procesos, es decir, ampliar el alcance de los mismos, tomando en cuenta la criticidad de los mismos para el negocio, permitiendo incluir a toda la empresa en un plan futuro de continuidad de negocio.
- Tomar el presente proyecto como base para proceder a la implementación del mismo con apoyo de especialistas y del uso adecuado y pertinente de tecnologías de información.
- Luego de realizadas sesiones de prueba y monitoreo de resultados, muy seguramente los altos ejecutivos o los encargados de la instauración de este proceso sabrán que han alcanzado el éxito cuando se sientan seguros que su organización puede responder a una crisis al sentirse capaces de garantizar la seguridad de los empleados, preservar los activos de IT, relanzar pronto las operaciones críticas y esenciales y controlar la interrupción de operaciones tanto IT, como de otras áreas relacionadas con la continuidad de las operaciones

Desarrollo e implementación de una metodología de gestión de incidente, ya que con las estrategias planteadas a lo largo del presente análisis y acorde a la elaboración de un Plan de Manejo de Crisis, queda abierta la posibilidad de definir políticas y procedimientos para la gestión de evento de TI, que suelen suceder de manera diaria sin llegar a ser una crisis.

6 REFERENCIAS

[1] AVALUTION CONSULTING (2012) ABOUT BUSINESS CATALYST SOFTWARE.USA: AVALUTION.

[2] BCI BUSINESS CONTINUITY INSTITUTE (2013) GOOD PRACTICE GUIDELINES 2013. EDICIÓN GLOBAL. REINO UNIDO: BCI.

[3] BUSINESS CONTINUITY INSTITUTE (BCI) (2007) BCI 2007. A MANAGEMENT GUIDE TO IMPLEMENTING GLOBAL GOOD PRACTICE IN BUSINESS CONTINUITY MANAGEMENT (CONSULTA: 26 DE AGOSTO DE 2015) ([HTTP://WWW.THEBCI.ORG/GPG2008V1%20SECTION6.PDF](http://www.thebci.org/gpg2008v1%20section6.pdf))

[4] BSI GROUP. ¿EN QUÉ PUNTO SE ENCUENTRA EN SU CAMINO HACIA LA ISO 22301: GESTIÓN DE CONTINUIDAD DE NEGOCIO? (CONSULTA: 26 DE AGOSTO DE 2015) ([HTTP://WWW.BSIGROUP.COM/ES-ES/ISO-22301-CONTINUIDAD-DE-NEGOCIO/](http://www.bsigroup.com/es-es/iso-22301-continuidad-de-negocio/)).

[5] CHAMBERS, ROBINSON (2014) BUSINESS CONTINUITY PLANNING: A PROJECT MANAGEMENT APPROACH. CALIFORNIA: AUERBACH PUBLICATIONS.

DRI DISASTER RECOVERY INSTITUTE (2012) A CULTURE OF BUSINESS CONTINUITY. DISASTER RECOVERY JOURNAL. NUEVA YORK.

[6] FULMER, KENNETH (2004) BUSINESS CONTINUITY PLANNING: A STEP BY STEP GUIDE WITH PLANNING FORMS. MONTANA: ROTHSTEIN PUBLISHING.

INTERNATIONAL ORGANIZATION FOR STANDARIZATION (ISO) (2012) ISO 22301:2012. SISTEMA DE GESTIÓN Y CONTINUIDAD DE NEGOCIO (CONSULTA:

05 DE MAYO DE 2015) ([HTTPS://WWW.ISO.ORG/OBP/UI/#ISO:STD:ISO:22301:ED-1:V2:EN](https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-1:v2:en))

[7] FLYNN, STEPHEN (2007) THE EDGE OF DISASTER: REBUILDING A RESILIENT NATION. USA: RANDOM HOUSE.

[8] HOTCHKISS, STUART (2010) BUSINESS CONTINUITY MANAGEMENT: A PRACTICAL GUIDE. REINO UNIDO: BCS, THE CHARTERED INSTITUTE FOR IT.

[9] IBM INTERNATIONAL BUSINESS MACHINES (2012) HOW SECURITY AND BUSINESS CONTINUITY CAN SHAPE THE REPUTATION AND VALUE OF YOUR COMPANY. USA: IBM.

[10] INTERNATIONAL STANDAR ORGANIZATION 22301:2012 SOCIETAL SECURITY – BUSINESS CONTINUITY MANAGEMENT SYSTEM – REQUIREMENTS. SUIZA: ISO.

[11] SANI SYSADMIN AUDIT NETWORKING AND SECURITY INSTITUTE (2005) THE DISASTER RECOVERY PLAN. USA: SANI. DELOITTE GLOBAL SERVICES LIMITED.

[12] SHARP, JOHN (2012) THE ROUTE MAP TO BUSINESS CONTINUITY MANAGEMENT: MEETING THE REQUIREMENTS OF ISO 22301. REINO UNIDO: THE BRITISH STANDARDSINSTITUTION.

[13] SUNGARD AVAILABILITY SERVICES (2011) LDRPS: LIVING DISASTER RECOVERY PLANNING SYSTEM. USA: SUNGARD.

[14] TUPIA, MANUEL (2011) PRINCIPIOS DE AUDITORÍA Y CONTROL DESISTEMAS DE INFORMACIÓN. SEGUNDA EDICIÓN. LIMA: TUPIA CONSULTORES Y AUDITORES S.A.C.

[15] WILLIAM, JON (2010) DISASTER RECOVERY PLANNING: SAVY BUSINESS CONTINUITY. NEW YORK: PEARSON PRENTICE HALL COMPUTIN.

[16] [HTTP://WWW.ISOTOOLS.PE/NORMA-ISO-22301/](http://WWW.ISOTOOLS.PE/NORMA-ISO-22301/)

[17] [HTTP://PECB.ORG/ISO22301ES/](http://PECB.ORG/ISO22301ES/)

[18] [HTTP://WWW.BVINDECOPI.GOB.PE/NORMAS/ISOIEC17799.PDF](http://WWW.BVINDECOPI.GOB.PE/NORMAS/ISOIEC17799.PDF)

[19] [HTTPS://WWW.DRII.ORG/CERTIFICATION/PROFESSIONALPRAC_SPANISH.PHP](https://WWW.DRII.ORG/CERTIFICATION/PROFESSIONALPRAC_SPANISH.PHP)

[20] [HTTP://SEMANAECONOMICA.COM/ARTICLE/SECTORES-Y-EMPRESAS/EDUCACION/199251-UPC-LA-UNIVERSIDAD-QUE-FINANCIO-TRES-CAMPUS-EN-4-ANOS-A-COSTA-DE-SU-DEUDA/](http://SEMANAECONOMICA.COM/ARTICLE/SECTORES-Y-EMPRESAS/EDUCACION/199251-UPC-LA-UNIVERSIDAD-QUE-FINANCIO-TRES-CAMPUS-EN-4-ANOS-A-COSTA-DE-SU-DEUDA/)

[21] [HTTP://WWW.SISTESEG.COM/FILES/DOCUMENTOMETODOLOGIABCPYDRP.PDF](http://WWW.SISTESEG.COM/FILES/DOCUMENTOMETODOLOGIABCPYDRP.PDF)

[22] [HTTPS://WWW.INCIBE.ES/PROTEGE-TU-EMPRESA/QUE-TE-INTERESA/PLAN-CONTINGENCIA-CONTINUIDAD-NEGOCIO](https://WWW.INCIBE.ES/PROTEGE-TU-EMPRESA/QUE-TE-INTERESA/PLAN-CONTINGENCIA-CONTINUIDAD-NEGOCIO)

[23][HTTPS://APECMSMEMARKETPLACE.COM/SITES/DEFAULT/FILES/DOC/BCP_GUIDEBOOK_ABRIDGED_VERSION_SPANISH_20140829.PDF](https://APECMSMEMARKETPLACE.COM/SITES/DEFAULT/FILES/DOC/BCP_GUIDEBOOK_ABRIDGED_VERSION_SPANISH_20140829.PDF)

[24][HTTP://DSpace.UDLA.EDU.EC/BITSTREAM/33000/5423/1/UDLA-EC-TMGSTI-2016-07.PDF](http://DSpace.UDLA.EDU.EC/bitstream/33000/5423/1/UDLA-EC-TMGSTI-2016-07.PDF)

[25][HTTPS://WWW.CISCO.COM/C/EN/US/PRODUCTS/COLLATERAL/SERVICES/HIGH-AVAILABILITY/WHITE_PAPER_C11-453495.PDF](https://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-453495.pdf)

[26][HTTPS://WWW.ALHAMBRA-EIDOS.COM/ES/DISASTER-RECOVERY-PLAN.HTML](https://www.alhambra-eidos.com/es/disaster-recovery-plan.html)

[27][HTTPS://WWW.PORTLAND.EU/HUBFS/VENDOREN/ACRONIS/ACRONIS%20WHITEPAPER%20HOW%20TO%20DEVELOP%20AN%20EFFECTIVE%20IT%20DISASTER%20RECOVERY%20PLAN.PDF](https://www.portland.eu/hubfs/Vendoren/Acronis/Acronis%20Whitepaper%20How%20to%20develop%20an%20effective%20IT%20disaster%20recovery%20plan.pdf)

[28][HTTP://WWW.SISTESEG.COM/FILES/MICROSOFT_WORD_-_METODOLOGIA_PLAN_RECUPERACION_ANTE_DESASTRES_DRP.PDF](http://www.sisteseq.com/files/microsoft_word_-_metodologia_plan_recuperacion_ante_desastres_drp.pdf)

[29][HTTP://WWW.BSCCONSULTORES.CL/DESCARGAS/D.5%20%20CONTINUIDAD%20DEL%20NEGOCIO%20Y%20%20RECUPERACIN%20DE%20DESASTRES%20ISACA.PDF](http://www.bscconsultores.cl/Descargas/D.5%20CONTINUIDAD%20DEL%20NEGOCIO%20Y%20RECUPERACION%20DE%20DESASTRES%20ISACA.PDF)

[30][HTTPS://WWW.TALENTIS.CL/CURSOS/GESTION-DE-SERVICIOS-TI/WORKSHOP-DRP-PLAN-DE-RECUPERACION-ANTE-DESASTRES/](https://www.talentis.cl/cursos/gestion-de-servicios-ti/workshop-drp-plan-de-recuperacion-ante-desastres/)

GLOSARIO

Continuidad: Supervivencia de los sistemas ante un desastres.

Desastre: Evento no predecible causado por la naturaleza o el factor humano.

Activo de información: Toda información que la entidad posee dentro de un activo informático como servidores, switch, etc. o por documentos como contratos, cotizaciones, etc.

Registros vitales: Información de clasificación confidencial de la empresa, que su divulgación podría comprometer la supervivencia de la empresa.

Mitigación: Conjunto de medidas para minimizar el impacto destructivo de un desastre.

Disaster Recovery Plan: Se refiere al plan de recuperación de desastres.

Contingencia: Posibilidad de que una cosa suceda o no suceda, riesgo, peligro, evento.

Emergencia: Estado excepcional de una comunidad amenazada o afectada por un desastre, el cual implica la aplicación de medidas de prevención, protección y control sobre los efectos del riesgo.

Información: Conjunto organizado de datos, los cuales constituyen un mensaje sobre determinado ente o fenómeno.

Proceso: Conjunto de las fases sucesivas de un fenómeno natural o de una operación artificial.

Actividad: Conjunto de procesos desarrollados por la organización que soporta uno o más productos o servicios.

Continuidad de negocio: Capacidad de la organización de continuar entregando productos o servicios a niveles aceptables predefinidos después de un evento alterador.

Bussiness Impact Analysis: Proceso de análisis de funciones organizaciones y el efecto de una interrupción en ellas.

Infraestructura: Conjunto de equipos y servicios necesarios para la operación de una organización.

Riesgo: Efecto de la incertidumbre y objetivos.

Recursos: Todos los activos, personas, destrezas, información, tecnología, locales.

Pruebas: Procedimiento para evaluar, un medio de determinar la presencia, calidad o veracidad de algo.

SIGLARIO

UPC: Universidad Peruana de Ciencias Aplicadas.

DRP: Disaster Recovery Plan.

TI: Tecnologías de la Información.

BIA: Business Continuity Plan.

BCI: Business Continuity Institute.

DRI: Disaster Recovery Institute.

ISACA: Information Systems Audit and Control Association.

ISO: International Organization for Standardization.

BSI: British Standards Institution.

NIST: National Institute Of Standards and Technology.

NFPA: National Fire Protection Association.

CCA: Centro de Cómputo Alterno.

CCP: Centro de Cómputo Principal.

ISCP: Information System Contingency Planning

POC: Point Of Contact

7. ANEXOS

CNTG-REH-01 PROCEDIMIENTO DE RESPUESTA EN CASO DE PÉRDIDA DE LOCAL PRINCIPAL

Objetivo

Recuperar la capacidad operativa, en el caso que el local principal de la universidad sufra alguna contingencia que imposibilite el funcionamiento del servicio.

Responsabilidades

El Equipo de Sistemas conformado por personal externo de soporte técnico, es responsable de ejecutar los procedimientos necesarios para restaurar el equipo, el software y las aplicaciones en el menor tiempo posible.

Procedimiento CNTG-REH-01

SEC	EQ	DESCRIPCION	REF
1	ES	Comunicar la contingencia al centro alternativo de acuerdo al procedimiento establecido	Anexo B
2	ES	Contactar al personal de custodia de Backup y solicitar el envío de las cintas en los maletines al centro alternativo.	Anexo C
3	ES	Coordinar con Proveedores de comunicaciones del cambio de dirección de los circuitos digitales al centro alternativo.	
4	EC	Proveer dirección y números telefónicos del centro alternativo a los equipos de recuperación.	Anexo A y B
5	EA	Proveer medio de transporte para el traslado del personal, equipos y suministros hacia el centro alternativo.	

SEC	EQ	DESCRIPCION	REF
6	EG	Manejar las actividades relacionadas con entrevistas públicas y ruedas de prensa motivadas por la contingencia.	
7	ES	Coordinar la configuración de los equipos de telecomunicaciones.	
8	ES	Instalar y configurar software base en Servidores del centro alternativo.	Anexo E
9	ES	Instalar y configurar las estaciones de trabajo.	Anexo E
10	ES	Ejecutar el proceso de restauración de los registros vitales y de los respaldos que se remitieron de la bóveda externa.	Anexo C
11	ES	Verificación de recepción adecuada de señal de los circuitos digitales.	
12	EA	Coordinar el traslado de usuarios al centro alternativo, efectuando actividades correspondientes como renta de transporte, comida rápida, mensajería, etc.	Anexo A
13	EU	Recibir y validar la información que requiere para su operación (traída de bóveda).	
14	EC	Coordinar y controlar situaciones que afecten las actividades de los equipos de recuperación por medio de acuerdos efectuados periódicamente, dependiendo la situación que prevalezca durante la contingencia.	

SEC	EQ	DESCRIPCION	REF
15	EU	Ingreso de data huérfana, trabajada en base a los procedimientos manuales.	Anexo F

Preparación y retorno al centro primario

SEC	ACT	DESCRIPCION	REF
16	EA	Listar el equipo y las instalaciones que resultaron dañadas durante la contingencia para su reparación o sustitución	Anexo D
17	EC	Prioriza adquisición o reparación de bienes afectados.	
18	EA	Cotiza reemplazo o reparación de equipo e instalaciones dañadas.	
19	EC	Valida cotización preparada.	
20	EG	Revisar y aprobar la inversión para la adquisición y/o reparación necesaria	
21	EA	Coloca las órdenes de compra según la inversión aprobada.	
22	EA	Supervisa a los diferentes proveedores en la instalación y adecuación de los bienes adquiridos.	
23	ES	Supervisa a los diferentes proveedores en la instalación y adecuación de los equipos adquiridos.	
24	ES	Respaldar la información procesada en el centro alternativo de acuerdo a los procedimientos establecidos y revisar que terminen en forma correcta	Anexo C

SEC	ACT	DESCRIPCION	REF
25	ES	Restaurar la información en instalaciones de la universidad.	Anexo C
26	EC	Declarar terminada la contingencia de la universidad, notificarlo a los equipos de recuperación y hacer entrega del equipo al centro alterno	
27	EU	Reanudar las operaciones en las instalaciones de universidad.	
28	EG	Comunicar a los clientes y proveedores la normalización del servicio.	Anexo A
29	EG	Comunica a la región la normalización de las actividades y presenta el reporte correspondiente.	

CNTG-REH-02 PROCEDIMIENTO DE RESPUESTA EN CASO DE PÉRDIDA DE EQUIPOS CRÍTICOS

Objetivo

El cambio o reparación efectiva y confiable del equipamiento considerado crítico para devolver el mismo a su estado de operación normal en el menor tiempo posible.

Responsabilidades

Es responsabilidad del Equipo Coordinador realizar el seguimiento al cumplimiento del presente procedimiento.

El Equipo de Sistemas conformado por el personal externo de soporte técnico, es responsable de efectuar la reparación y puesta en operatividad de los equipos.

Procedimiento CNTG-REH-02

SEC	EQ	DESCRIPCION	REF
1	EC	Se encargará de contactar a todo el personal de soporte involucrado en el esfuerzo de reposición	Anexo A
2	ES	Realiza el diagnóstico y detección de la falla en el equipo.	
3	ES	Determina el grado de pérdida, el impacto de la misma y las acciones a tomar dependiendo del grado de contingencia y se informa al Equipo Coordinador	
4	ES	En caso se requiera el traslado al Centro Alterno se debe ejecutar el <i>Procedimiento CNTG-REH-01</i>	
5	ES	En caso se requiera reparación o cambio del equipo se coordina con el proveedor correspondiente	Anexo A

SEC	EQ	DESCRIPCION	REF
6	EC	Según sea el caso, se activan los procedimientos manuales DRP de los procesos afectados	
7	ES	Una vez solucionado el problema se procede a la instalación y configuración de las aplicaciones y servicios brindados	Anexo C
8	ES	Solicita los backups y los restablece	Anexo C
9	ES	Realiza las pruebas de funcionamiento necesarios	
10	EU	Realiza la digitación de la data Huérfana en los sistemas restablecidos. (Si hubiese)	
11	EG	Comunica a la región la normalización de las actividades y presenta el reporte correspondiente.	

CNTG-REH-03 PROCEDIMIENTO DE RESPUESTA EN CASO DE PÉRDIDA DE SOFTWARE BASE Y APLICACIONES

Objetivo

El restablecimiento del Software y aplicaciones relevantes en el menor tiempo posible, ante un evento en el cual el software base y/o las aplicaciones se dañen o corrompan.

Responsabilidades

Es responsabilidad del Equipo Coordinador controlar el cumplimiento del presente procedimiento.

El personal de soporte técnico se encargará de ejecutar los procedimientos necesarios para restaurar, reinstalar o reconfigurar el software dañado o perdido.

Procedimiento CNTG-REH-03

SEC	EQ	DESCRIPCION	REF
1	EC	Se encargará de contactar a todo el personal de soporte involucrado en el esfuerzo de reposición	Anexo A
2	ES	Realiza el diagnóstico y detección del origen del problema.	
3	ES	Determina el grado de pérdida, el impacto de la misma y las acciones a tomar dependiendo del grado de contingencia y se informa al Equipo Coordinador	
4	ES	En caso se requiera el traslado al Centro Alterno se debe ejecutar el <i>Procedimiento CNTG-REH-01</i>	
5	ES	En caso se requiera reparación o cambio del equipo se debe ejecutar el <i>Procedimiento CNTG-REH-02</i>	
6	ES	Una vez solucionado el problema se procede a la instalación y configuración de los equipos afectados	Anexo C
7	ES	Solicita los backups y los restablece	Anexo C
8	ES	Realiza las pruebas de funcionamiento necesarios	
9	EU	Realiza la digitación de la data Huérfana en los sistemas restablecidos (Si hubiese).	

SEC	EQ	DESCRIPCION	REF
10	EG	Comunica a la región la normalización de las actividades y presenta el reporte correspondiente.	

ANEXO A

Personal participante durante la reunión.

Nombre	Dirección	Teléfono oficina / anexo	Teléfono particular	Celular
Equipo Gerencial				
Luis Miguel Velásquez Castañeda (Lider)				994611366
William Romero Solís (Alternó)				997566235

Nombre	Dirección	Teléfono oficina / anexo	Teléfono particular	Celular
Equipo Coordinador				
Henry Longa Alegria (Lider)				997556234
William Romero Solís (Alterno)				997566235
Humberto Carranza (Integrante)				989048909
Lea Sulmont (Integrante)				989048891
Milagros Morgan (Integrante)				994611368
Ángel Liu (Integrante)				994616448
Teresa Rivera (Integrante)				986629811
Jose Almeza (Integrante)				997599803
Demetrio Elgueta (Integrante)				994611363
Tomas Tapia (Integrante)				994611369
Blanca Zavaleta (Integrante)				997566233
Jorge Rivera (Integrante)				997566232
Oscar Flores (Integrante)				993531866
Guillermo Quiroga (Integrante)				944483921
Rodolfo Cremer (Integrante)				989048905
Marysol Suarez (Integrante)				

Nombre	Dirección	Teléfono oficina / anexo	Teléfono particular	Celular
Equipo de Sistemas				
Jorge Navarro Price (Lider)				997593223
Úrsula Sánchez Tejada (Alternó)				993534085
Jorge Nako Oshiro (Integrante)				997596869
Miguel Patiño Motta (Integrante)				997566242

Nombre	Dirección	Teléfono oficina / anexo	Teléfono particular	Celular
Equipo de Apoyo Administrativo				
William Romero Solís (Lider)				997566235
Henry Longa Alegría (Alternó)				997566234
Liliana Carranza (Integrante)				993526088
Shirley Villanes (Integrante)				997592530

Listado de contactos de emergencia.

LISTA DE CONTACTOS PARA EMERGENCIAS

TIPO	EMPRESA	NOMBRE DE CONTACTO	CORREO	TELEFONO
Servidores	Casaqui Data	Carlos Valverde	cvalverde@casapiata.com.pe	215-4530 - 99 35 47 409
	JMLD	Nelson Damazo	nelson.damazo@jml.com.pe	9975 04 533
	Adeco del Perú	Marta Jesús Uribe Ariza	murbe.ariza@adex.com.pe	9975 01 335
Bite - SAN	HP	Fabian Salazar	fabiansalazar@hp.com	98240034
Upe	OIC Ing.	Juan José Leira	jleira@oic.com.pe	9996 56 389 - 551 0729
Backup	Storage Data	Rafel Figueroa Ruiz	rafel.figueroa@storage.com.pe	221-7193 - 99 0007 389
	JMLD	Nelson Damazo	nelson.damazo@jml.com.pe	9975 04 533
	Backup	Jorge Castillo Rey	jcastillo@backup.com.pe	224-0896
Switch 3COM	System Support Services	Sara Saez Rodriguez	saezrod@ass.com.pe	9935 06 029
Switch Cisco	Casaqui Data	Carlos Valverde	cvalverde@casapiata.com.pe	215-4530 - 99 35 47 409
	Adeco del Perú	Marta Jesús Uribe Ariza	murbe.ariza@adex.com.pe	9975 01 335
	Cisco	Julio Gonzalez	juliocon@cisco.com	9916 06 036 - 255 51 49
Enlace a Internet / Datos	Claro	Gladya Pérez, Estelina - Gerente Operativa	gladya.perez@claro.com.pe	6102 081 - 99752 1928
		Mirko Lallier - Gerente de Ventas	mirko.lallier@claro.com.pe	6102 058 - 99751 0071
		Reportes	Central.Reporte.de.incidentes	6102 273
MS Microsoft	System Support Services	Sara Saez Rodriguez	saezrod@ass.com.pe	9935 06 029
	Casaqui Data	Carlos Valverde	cvalverde@casapiata.com.pe	215-4530 - 99 35 47 409
	ITG Solutions	Manuel Murayo	manuel.murayo@itgsolutions.com.pe	6284 404 - 99463 1504
Oracle	Oracle Perú	Glenda Prieta Díaz	glenda.prieta@oracle.com	7118981 - 99276 8192
	IT Group	Carlos Talcazo	ctalcazo@itgroup.com.pe	2211 385 - 99936 3961
	GIS	Miguel Palacios	miguel.palacios@gis.pe	9935 00992 - 7084609
	Red Partner	Ricardo Cardenas	ricardo.cardenas@redpartner.com.pe	6404 002 - 96176 3093
Spring	Royal Systems	Carlos Alaya	calaya@royalsystems.com.pe	422-4415
Autodesk	SoftLand	Miguel Wainy	miguelwainy@softland.com	9941 08494 - 4416144
Telefonía	Telefonía	Carlos Jiménez Aguilera	carlos.jimenez@telefonica.com	9999 29324 - 2109393
Central Telefonía	Surtec	Jorge Lay	jorge.lay@surtecperu.com	7054300
	Belltech	Renzo Zavalta	renzo.zavalta@belltech.com.pe	6112907
	SSLS	Sara Saez Rodriguez	saezrod@ass.com.pe	9935 06 029
Sistema Elección	UPC	Rafel Eche	rafel@upc.edu.pe	9975 97 060
	OIC Ing.	Juan José Leira	jleira@oic.com.pe	9996 56 389 - 551 0729
Enlace a la Fibra	EBD	Diego Maza	dmaza@ebdperu.com	988168561
	Telco Services	Armando Basora	arbasora@telcoservices.com.pe	9823 3866 / 97912 310
Firewall Checkpoint	Casaqui Data	Carlos Valverde	cvalverde@casapiata.com.pe	215-4530 - 99 35 47 409
WiFi - Access Point	Casaqui Data	Carlos Valverde	cvalverde@casapiata.com.pe	215-4530 - 99 35 47 409
	Adeco del Perú	Marta Jesús Uribe Ariza	murbe.ariza@adex.com.pe	9975 01 335
WWW	Migla	Juan José Miranda del Solar	jsolar@miglatel.com	221-3653
Mailbox	E-Target	Javier Inojosa	jinojosa@interzonetel	4368015 - 97908 496
Aleja	Sistema Argos	Alfredo Benavides	benavides@argos.com.mx	452 55 52 54 5352
Manilla	Autarica	Alfredo Zentillo	alfredozentillo@autarica.com	7151 072
Autopagos	Casaqui Data	Carlos Valverde	cvalverde@casapiata.com.pe	215-4530 - 99 35 47 409