UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

FACULTAD DE INGENIERIA

PROGRAMA ACADÉMICO DE INGENIERÍA DE REDES Y COMUNICACIONES

Diseño de un plan de recuperación ante desastres basado en la norma NIST SP 800-34 rev1 para un proveedor de servicios de telecomunicaciones en el Perú

TESIS

Para optar el título profesional de Ingeniero de Redes y Comunicaciones

AUTOR

Cuta Benites, Edward Wilbert (0000-0001-6007-0244)

ASESOR

Flores Solis, Fernando Rolyn (0000-0002-6105-3371)

Lima, 26 de febrero de 2020

DEDICATORIA

La presente tesis va dedicado a mis padres quienes se esforzaron mucho para que yo me convirtiera en un profesional, y me inculcaron los valores necesarios para ser una persona de bien; También va dedicado a mi familia quienes siempre me motivaron para seguir adelante en mis metas trazadas; por último, agradecer a mis amigos y colegas que me apoyaron con sus consejos y experiencias para poder realizar el presente trabajo.

RESUMEN

El presente trabajo tiene como objetivo desarrollar un plan de recuperación ante desastres para una empresa peruana de telecomunicaciones, tomando como un marco de referencia a la norma americana NIST 800-34, para ello se siguió los 7 procesos de planificación de contingencias que sugiere la norma.

El trabajo está compuesto por 11 capítulos, en los tres primeros capítulos se hacen un acercamiento a la organización con el fin de conocer la estructura interna en el que se explora las situaciones problemáticas que afronta la organización, así mismo se definen los objetivos que serán clave para el desarrollo de todo el proyecto, en el marco teórico se analiza a fondo los procesos de la norma y los conceptos necesarios para comprender el tema. En el capítulo 4 se desarrolla ampliamente el plan de recuperación ante desastres, para ello se hace un análisis de impacto de negocio con el que se logra determinar los tres procesos críticos del negocio, como parte de este proceso se realiza un análisis de riesgo de todos los recursos que intervienen en los procesos críticos, dicho análisis sirve de entrada para definir los seis escenarios de desastre, así mismo se desarrollaron las estrategias que permitan actuar ante dichos escenarios, se definen los recursos necesarios, los roles y responsabilidades de los equipos de respuesta, por otro lado se realizaron pruebas y ejercicios de los sistemas implementados para garantizar su eficacia ante un escenario real.

Por último, se hace un análisis de los resultados y se brinda las conclusiones y recomendaciones.

Palabras clave**:** DRP; BIA; análisis de riesgos; desastre, continuidad, estrategias de contingencia.

Design of a disaster recovery plan based on the NIST SP 800-34 rev1 standard for a telecommunications service provider in Peru

ABSTRACT

This paper aims to develop a disaster recovery plan for a Peruvian telecommunications company, taking as a frame of reference the American standard NIST 800-34, for this the 7 contingency planning processes suggested by the standard were followed.

The work is composed of 11 chapters, in the first three chapters an approach to the organization is made in order to know the internal structure in which the problematic situations that the organization faces are explored, as well as defining the objectives that will be key For the development of the entire project, in the theoretical framework the processes of the standard and the concepts necessary to understand the subject are thoroughly analyzed. In Chapter 4, the disaster recovery plan is widely developed as such, for this a business impact analysis is made with which it is possible to determine the three critical processes of the business, as part of this process a risk analysis of all assets is performed that intervene in the critical processes, this analysis serves as input to define the six disaster scenarios, as well as the strategies that allow acting in these scenarios, the necessary resources, roles and responsibilities of the response teams are defined, by On the other hand, tests and exercises of the systems implemented were carried out to guarantee their effectiveness in a real scenario.

Finally, an analysis of the results is made, and the conclusions and recommendations are provided.

Keywords: DRP; BIA; risk analysis; disaster, continuity, contingency strategies.

TABLA DE CONTENIDOS

1 ASPECTOS INTRODUCTORIOS 1

1.1 ORGANIZACIÓN OBJETIVO 1

1.2 CAMPO DE ACCIÓN DE LA ORGANIZACIÓN OBJETIVO 2

1.3 SITUACIÓN PROBLEMÁTICA 4

1.4 IDENTIFICACIÓN DEL PROBLEMA 5

1.5 OBJETIVOS 5

1.5.1 Objetivo general 5

1.5.2 Objetivos específicos 5

1.6 INDICADORES DE LOGRO DE OBJETIVOS 6

1.7 JUSTIFICACIÓN DEL PROYECTO 6

1.8 ESTADO DEL ARTE 7

1.8.1 Conceptos clave de continuidad de negocio 8

1.8.2 Evolución de normas y estándares 9

1.8.3 Instituciones 17

1.8.4 Tendencia en los DRP 19

2 MARCO TEORICO 21

2.1 CONCEPTOS GENERALES 21

2.2 PROCESO DE PLANIFICACIÓN NIST 800-34 22

2.2.1 Desarrollar la política de planificación de contingencias: 22

2.2.2 Realizar el análisis de impacto de negocio (BIA) 23

2.2.3 Identificar controles preventivos 29

2.2.4 Crear estrategias de contingencia 30

2.2.5 Plan de pruebas, entrenamiento y ejercicios TT&E (Plan Testing, Training, and Exercises). 33

2.3 ANÁLISIS DE RIESGOS 36

2.3.1 Metodología para el análisis de riesgos 37

3 DEFINICIÓN DEL PROBLLEMA 41

3.1 ANÁLISIS DEL PROBLEMA 41

3.2 INTERESADOS 45
3.3 EDT 49
4 DISEÑO DE LA SOLUCIÓN 50
4.1 POLÍTICA DE PLAN DE RECUPERACIÓN ANTE DESASTRES 50
4.2 ANÁLISIS DE IMPACTO DE NEGOCIO BIA 53
4.3 ANÁLISIS DE RIESGOS 59
4.3.1 Identificación de recursos 59
4.3.2 Evaluación de riesgos: 62
4.3.3 Tratamiento de riesgos 68
4.3.4 Riesgos residuales 70
4.4 CONTROLES PREVENTIVOS 71
4.5 ESCENARIOS DE DESASTRE 71
4.6 ESTRATEGIAS DE CONTINGENCIAS 74
4.7 PROCESO DE EJECUCIÓN DE DRP 80
4.8 RECURSOS 82
4.9 ROLES Y RESPONSABILIDADES 86
4.10 ÁRBOL DE COMUNICACIONES 89
4.11 ACTIVIDADES DE PRUEBA, EJERCICIO Y ENTRENAMIENTO TT&E 91
4.11.1 Escenario de prueba: Falla de DC principal 91
4.11.2 Pruebas de Mitigación de ataques de tipo DDoS. 103
4.11.3 Pruebas de redundancia de proveedores de internet: 106
4.11.4 Ensayo de TAC y NOC alterno. 109
4.12 PLAN DE MANTENIMIENTO 112
5 PRUEBAS, RESULTADOS Y VALIDACIÓN 114
5.1 PLAN DE PRUEBAS (PARA EL OE1) 115
5.1.1 Propósitos de la evaluación 115
5.1.2 Alcance de evaluación 115
5.1.3 Recursos para las pruebas 115
5.1.4 Estrategia de verificación 115
5.1.5 Diagrama de actividades 116
5.1.6 Casos de prueba de uso 116
5.1.7 Objetivos del indicador 118

5.2 PLAN DE PRUEBAS (PARA EL OE2) 118
5.2.1 Propósitos de la evaluación 118
5.2.2 Alcance de la evaluación 119
5.2.3 Recursos para las pruebas 119
5.2.4 Estrategia de verificación 119
5.2.5 Diagrama de actividades 119
5.2.6 Casos de prueba de uso 120
5.2.7 Objetivos del indicador 121
5.3 PLAN DE PRUEBAS (PARA EL OE3) 122
5.3.1 Propósitos de la evaluación 122
5.3.2 Alcance de la evaluación 122
5.3.3 Recursos para las pruebas 123
5.3.4 Estrategia de verificación 123
5.3.5 Diagrama de actividades 123
5.3.6 Casos de prueba de uso 123
5.4 ANÁLISIS DE RESULTADOS DE PRUEBAS TT&E 126
5.4.1 Análisis de resultados de prueba 1 126
5.4.2 Análisis de resultados de prueba 2 127
5.4.3 Análisis de resultados de prueba 3 128
5.4.4 Análisis de resultados de prueba 4 129
6 CONCLUSIONES 131
7 RECOMENDACIONES 132
8 REFERENCIAS 133
9 GLOSARIO 135
10 SIGLARIO 136
11 ANEXOS 137

ÍNDICE DE TABLAS

Tabla 1 Indicadores de logro de objetivos 6
Tabla 2 Tabla de componentes de recursos 28
Tabla 3 Listado de personal especializado y sus funciones 41
Tabla 4 Documentación de procedimientos 42
Tabla 5 Listado de protocolos ausentes 42
Tabla 6 Reporte de averías por categorías en el primer semestre del año 2019 45
Tabla 7 Tabla de interesados 45
Tabla 8 Requerimientos alineados a los objetivos específicos 47
Tabla 9 Fases del BIA 53
Tabla 10 Procesos críticos y servicios 54
Tabla 11 Procesos de negocio y Tipo de impactos 55
Tabla 12 Leyenda análisis de BIA 55
Tabla 13 Porcentaje de facturación anual por proceso de negocio 56
Tabla 14 Pérdidas económicas de cada proceso de negocio por hora 56
Tabla 15 Valor de RPO por cada proceso de negocio. 56
Tabla 16 Valor de RTO para cada proceso de negocio 56
Tabla 17 Valor de WRT para cada proceso de negocio 57
Tabla 18 Factores para el cálculo de MTD por proceso de negocio 57
Tabla 19 Valores para el MTD por proceso de negocio. 58
Tabla 20 resumen de recursos y prioridades 58
Tabla 21 Inventario de recursos por nivel de criticidad. 59
Tabla 22 Leyenda de nivel de criticidad de los recursos. 61
Tabla 23 Evaluación de riesgos por procesos de negocio. 62
Tabla 24 Tratamiento de los riegos. 68
Tabla 25 Análisis de riesgos residuales. 70
Tabla 26 Escenario de desastre 1. 72
Tabla 27 Escenario de desastre 2. 72
Tabla 28 Escenario de desastre 3. 73
Tabla 29 Escenario de desastre 4 73
Tabla 30 Escenario de desastre 5 73
Tabla 31 Escenario de desastre 5 74
Tabla 32 Recursos necesarios para el escenario 1 82

Tabla 33 Recursos necesarios para el escenario 2 82
Tabla 34 Recursos necesarios para el escenario 3 83
Tabla 35 Recursos necesarios para el escenario 4 84
Tabla 36 Recursos necesarios para el escenario 5 84
Tabla 37 Recursos necesarios para el escenario 6 85
Tabla 38 Comité de crisis 86
Tabla 39 Equipo de respuesta de redes. 86
Tabla 40 Equipo de respuesta de Datacenter y Nodos 87
Tabla 41 Equipo de respuesta de Infraestructura 87
Tabla 42 Equipo de respuesta de Infraestructura de TI 87
Tabla 43 Equipo de respuesta de Legal y Capital Humano 89
Tabla 44 Equipo de respuesta de comunicaciones e imagen 89
Tabla 45 Árbol de comunicaciones 90
Tabla 46 plan de entrenamiento 111
Tabla 47 Formato de control de cambios 113
Tabla 48 Cronograma de mantenimiento del DRP 113
Tabla 49 Resumen de requisitos del objetivo 1 114
Tabla 50 Resumen de requisitos del objetivo 2 114
Tabla 51 Resumen de requisitos del objetivo 3 115
Tabla 52 Relación entre prueba 1, escenarios y procesos críticos. 126
Tabla 53 Evaluación de resultados prueba 1 126
Tabla 54 Relación entre prueba 2, escenario y procesos críticos. 127
Tabla 55 Evaluación de resultados prueba 2 127
Tabla 56 Relación entre prueba 3, escenario y procesos críticos. 128
Tabla 57 Evaluación de resultados prueba 3 128
Tabla 58 Relación entre prueba 3, escenario y procesos críticos. 129
Tabla 59 Evaluación de resultados prueba 4 129

ÍNDICE DE FIGURAS

Figura 1 Organigrama General de la organización objetivo..... 2
Figura 2 Organigrama de la dirección de operaciones 3
Figura 3 Ciclo de vida de BCM..... 10
Figura 4 Fases del modelo PDCA 13
Figura 5 comparación del cuadrante mágico de Gartner entre el año 2017 y 2018 20
Figura 6 Proceso de planificación de contingencia 22
Figura 7 Proceso de análisis de impacto de negocio 25
Figura 8 Punto de equilibrio de costo y tiempo de disrupción. 27
Figura 9 Proceso de análisis de riesgos 38
Figura 10 Reporte de ataques de tipo DDoS de 24 horas..... 43
Figura 11 Evidencia de ataques DDoS a la compañía.. 44
Figura 12 EDT..... 49
Figura 13 Flujo de ejecución de DRP..... 81
Figura 14 Diagrama de equipos CORE 92
Figura 15 Simulación de falla Equipo Core-INT 1 93
Figura 16 Verificación de role Router Core-INT 94
Figura 17 Verificación de secuencia de conmutación de roles. 94
Figura 18 Proceso de reinicio del módulo 5 vss 1..... 95
Figura 19 Comprobación de roles del sistema VSS 95
Figura 20 Validación de secuencia de cambio de roles..... 96
Figura 21 Validación de tarjetas encendidas 96
Figura 22 Verificación de tarjetas apagadas..... 97
Figura 23 Validación de conmutación de tráfico del proveedor Level 3 97
Figura 24 Validación de conmutación de tráfico del proveedor Telxius 98
Figura 25 Diagrama de escenario de falla Core-AGG 99
Figura 26 Validación de roles del sistema VSS Core-Agg 100
Figura 27 Validación de cambio de roles Core-Agg 100
Figura 28 Verificación de tarjetas encendidas Core-Agg..... 101
Figura 29 Apagado de tarjetas de equipo Core-Agg 101
Figura 30 Validación de redundancia de tráfico para nodo N001 102

Figura 31 Validación de redundancia de tráfico para nodo N021 102
Figura 32 Verificación del tráfico global, sin afectación 103
Figura 33 Detección de ataque DDoS 104
Figura 34 Notificación de mitigación Cloud 104
Figura 35 Consola de herramienta de mitigación Cloud 105
Figura 36 Notificación del evento vía correo 105
Figura 37 Notificación de fin de mitigación Cloud 106
Figura 38 Apagado de interfaz asociado al proveedor CenturyLink 107
Figura 39 Trafico asumido por interfaz asociado al proveedor Telxius 107
Figura 40 Apagado de interfaz asociado al proveedor Telxius 108
Figura 41 Trafico asumido por la interfaz asociada al proveedor CenturyLink 108
Figura 42 Personal en ensayo de TAC y NOC alterno Sede 1 109
Figura 43 Personal en ensayo de TAC y NOC alterno Sede 2 110
Figura 44 Plan de mantenimiento de DRP 112
Figura 45 Flujo de actividades para la comprobación del objetivo 1 116
Figura 46 Flujo de actividades para la comprobación del objetivo 2 119
Figura 47 Flujo de actividades para la comprobación del objetivo 3 123

1 ASPECTOS INTRODUCTORIOS

1.1 Organización Objetivo

La empresa en donde se enfoca este proyecto es una compañía de telecomunicaciones peruana que cuenta con 15 años de experticia en el sector corporativo peruano, cuyo objetivo principal es satisfacer las necesidades de sus clientes, a la fecha cuenta con más de 4000 clientes activos brindándoles servicios de Internet dedicado de banda ancha, transmisión de datos, streaming, telefonía fija, seguridad gestionada entre otros servicios informáticos, esta gran cantidad de servicios ofrecidos ha permitido atraer a clientes de diferentes sectores como como instituciones públicas, servicios de salud, call centers, construcción e inmobiliarias, minería, transportes, telecomunicaciones, carriers, entre otros.

Actualmente la empresa tiene una cobertura en las ciudades de Lima, Callao, Tacna, Trujillo, Chiclayo, Piura y Arequipa, habiendo desplegado más de 4500 km de fibra óptica, contando con 70 nodos pertenecientes a la Red Metro Ethernet[1] y MPLS[2], así mismo desde el 2006 es miembro del NAP y, desde el 2012, integrante del Consejo Directivo de la Asociación NAP Perú[3], que congrega a las más importantes empresas de telecomunicaciones del mercado peruano, a fin de servir de punto de intercambio de datos entre sus respectivas redes.

Ventaja competitiva:

Como ventaja competitiva la compañía cuenta con personal de soporte especializado propio en todos sus niveles, con lo cual le permite ahorrar costos en personal externo y consultorías.

Valor agregado:

Como parte del valor agregado la compañía ha agregado a su catálogo de servicios como el internet seguro que consiste en una solución de seguridad de firewall y UTM en la nube a costos competitivos.

Visión

Ser el mejor aliado estratégico en telecomunicaciones e internet del sector corporativo peruano.

---

[1] Arquitectura de red destinada a suministrar servicios sobre una red metropolitana. (Halabi, 2003)
[2] Mecanismo de transporte de datos estándar creado por la EITF definido en el RFC 3031
[3] Punto de interconexión neutral entre operadores de internet en el Perú.

Misión

Proveer servicios de alta tecnología acordes con las necesidades del mercado, adelantándonos a ellas en base a la pasión y talento de nuestros colaboradores, contribuyendo con el desarrollo sostenido del país.

Organigrama General:

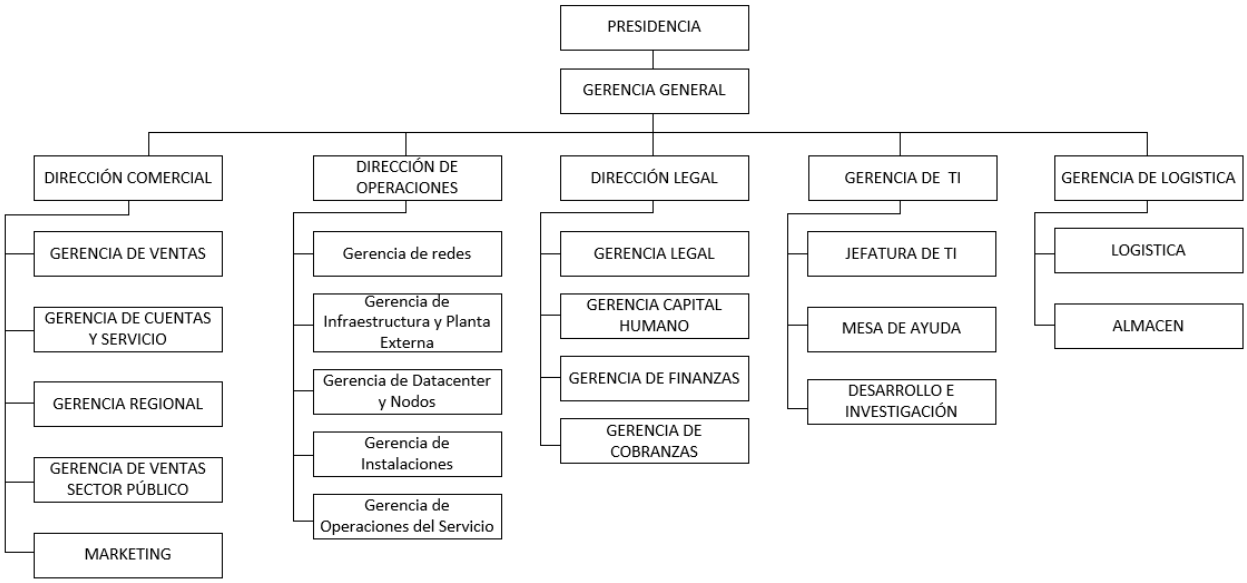


Figura 1 Organigrama General de la organización objetivo.
Fuente: Elaboración propia

1.2 Campo de acción de la organización objetivo

El campo de acción de la organización objetivo será la dirección de operaciones, que está compuesta por 5 gerencias y 15 áreas, cuyas principales funciones son:

Gerencia de Infraestructura y planta externa: en esta parte de la organización se realiza el diseño de la infraestructura de la planta externa, para el crecimiento de la red backbone y para el despliegue de la fibra óptica hasta la sede del cliente, así mismo brindan el servicio de mantenimiento a la planta externa cuando se producen averías.

Gerencia de redes: el área de ingeniería de red IP es la encargada de diseñar soluciones complejas para los clientes y homologar nuevos productos y servicios, por otro lado, se tiene el área de ingeniería core IP, quien es el encargado de diseñar e implementar soluciones a

nivel de backbone, así mismo el área NOC monitorea y da soporte a la red de manera continua 24 horas al día, 7 días a la semana (24x7).

Gerencia de datacenter y nodos: las principales funciones de esta gerencia es la construcción de la infraestructura de datacenters y nodos, así como custodiar su control de acceso, por otro lado, también son los encargados de dar soporte en todo lo relacionado a sistemas de energía eléctrica.

Gerencia de operaciones del servicio: en esta gerencia se encuentran las áreas de TAC y SOC, quienes son los que dan un soporte 24x7 de nivel 1 y nivel 2 a los clientes, en estas áreas se resuelven el 85% de los casos reportados por los clientes.

La red backbone está compuesta por 70 nodos, a su vez estos nodos pertenecen a dos redes (Metro Ethernet y MPLS) que trabajan en paralelo, así mismo se cuenta con 2 centros de datos que aloja a los servidores y equipos más críticos de la red.

A nivel de proveedores se cuenta con dos proveedores internacionales para el servicio de Internet, los cuales son Telxius y CenturyLink, con una capacidad de ancho de banda de 60 y 40 Gbps respectivamente, por otro lado, para poder brindar servicio a las provincias se cuenta como proveedores de transporte a Internexa y a la Red Dorsal Nacional de Fibra Óptica (RDNFO).

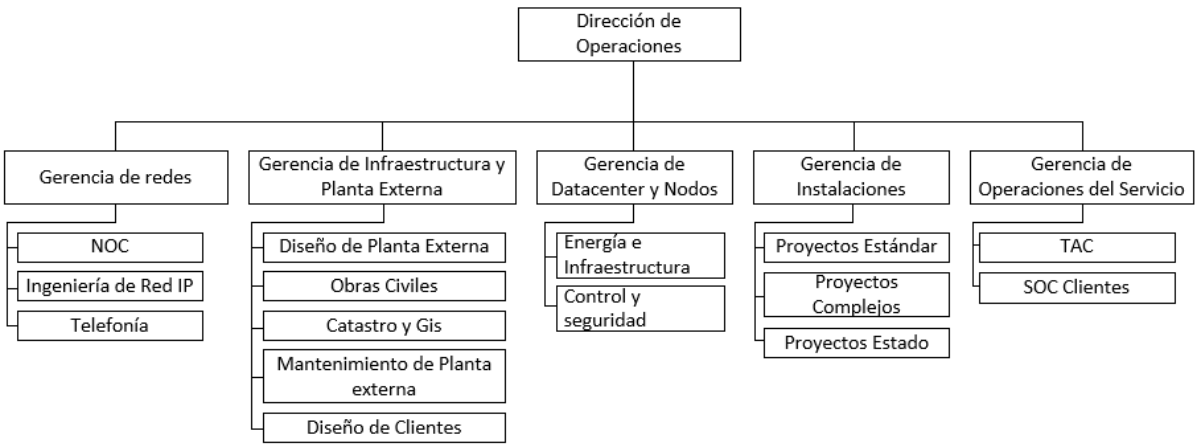


Figura 2 Organigrama de la dirección de operaciones

Fuente: Elaboración propia

1.3 Situación Problemática

La compañía durante los últimos 5 años ha afrontado eventos críticos que han impactado gravemente en la disponibilidad del servicio, esto se ve reflejado en el incumplimiento de los contratos de nivel de servicio (SLA por sus siglas en ingles), lo que conlleva a pérdidas económicas y daños a la imagen, estos eventos disruptivos han sido originados por diversos motivos tales como:

- Daños a la planta externa, la afectación se debió a que no hubo una comunicación previa por parte de la municipalidad, que ejecutó trabajos de demolición y rotura de pistas, afectando el canalizado de la fibra óptica, por otro lado, no se habían activado las rutas de contingencia, lo que dejó fuera de servicio casi el 50% de los nodos por más de 4 horas.
- Afectación a la red a causa de error humano, una falla en la configuración de un equipo de red generó una tormenta de broadcast, que inundó la red de capa 2 haciendo que los procesadores de los equipos de red se elevaran generando una interrupción de 30 minutos.
- Falla de energía eléctrica que afectó el centro de datos principal, ocasionado por la falla en los sistemas de respaldo de energía, dejando a la red fuera de servicio durante 1 hora.
- Falla hardware en las controladoras de equipos de Core, que generaron una inestabilidad en la red al no poder establecer roles de principal y secundario, generando intermitencias en la red por más de 30 minutos.
- Ataques de tipo de DDoS[4], provenientes de países como China, EE. UU y Rusia, aprovechando las vulnerabilidades en la red, ejecutaron ataques de fragmentación de IP, DNS amplification, LDAP amplification y NTP amplification[5], que generaron volúmenes de tráfico mayores a 50 Gbps, lo que ocasionó una saturación en las salidas internacionales impactando en el 60% de circuitos de internet.

[4] Ataques de red distribuidos que aprovecha los límites de capacidad de cualquier recurso de red. (Kaspersky, 2017)
[5] Ataques de tipo reflexión que aprovechan las vulnerabilidades del protocolo UDP para suplantar direcciones IP. (PCWorld, 2016).

Las acciones llevadas por los especialistas para la recuperación de los servicios ante un evento critico no se encuentran documentadas o existen de manera parcial, lo cual genera una dependencia del personal especializado.

Así mismo no se cuenta con un plan de pruebas y/o simulacros, tampoco se han identificado todos los escenarios que puedan afectar la continuidad del negocio de manera conjunta con todas las áreas involucradas en el negocio.

1.4 Identificación del problema

El problema identificado es que no se cuenta con un plan y estrategias de recuperación que garanticen razonablemente la continuidad de las operaciones de los procesos críticos, ante la ocurrencia de un evento disruptivo, esto debido a varios factores tales como: la falta de pruebas o simulacros que no permiten garantizar la eficiencia de los sistemas de contingencias; falta de documentación de los procedimientos críticos; falta de protocolos o políticas que se deban de cumplir ante un determinado escenario. Todos estos factores evidencian una vulnerabilidad en cuanto a la manera de afrontar una posible catástrofe, lo que podría desencadenar cuantiosas pérdidas económicas, afectación a la imagen y la reputación.

1.5 Objetivos

1.5.1 Objetivo general

Diseñar un plan de recuperación ante desastres, aplicando la norma NIST SP 800-34 rev1 que permita establecer estrategias de recuperación y garantizar la continuidad de las operaciones de los procesos críticos de un proveedor de servicios de telecomunicaciones en el Perú.

1.5.2 Objetivos específicos

Con el fin de poder lograr el objetivo general se requiere de poder cubrir los siguientes objetivos específicos.

- Identificar los procesos críticos de la compañía que permita calcular el impacto operacional y financiero, para su priorización ante un desastre.
- Identificar los escenarios y los riesgos críticos que puedan impactar el normal funcionamiento de los procesos críticos del negocio.
- Desarrollar estrategias y procedimientos de recuperación para los escenarios definidos.

1.6 Indicadores de logro de objetivos

Tabla 1 Indicadores de logro de objetivos

Objetivo Específico	Indicador de Logro	Métrica
Identificar los procesos críticos de la compañía que permita calcular el impacto operacional y financiero, para su priorización ante un desastre.	Análisis de impacto de negocio (BIA).	N° de procesos críticos. Cálculo de: RTO RPO MTD
Identificar los escenarios y los riesgos críticos que puedan impactar el normal funcionamiento de los procesos críticos del negocio.	Matriz de riesgos.	% de riesgos por nivel de criticidad
Desarrollar estrategias y procedimientos de recuperación para los escenarios definidos.	Informe de estrategias y procedimientos.	N° de estrategias por escenario. Eficiencia

Fuente: Elaboración propia.

1.7 Justificación del proyecto

El factor económico es uno de los puntos más importantes en cualquier organización, por lo que es necesario considerar una manera efectiva de salvaguardar los intereses de la compañía, mediante un plan de recuperación ante desastres se tiene garantía de que se puede afrontar una catástrofe con el menor impacto económico posible, esto se lleva a cabo desde el diseño del plan, en el que se calcula parámetros como el tiempo máximo de inactividad tolerable, lo que permite elaborar un contrato de nivel de servicio razonable, que no afecte de manera significativa a los ingresos de la compañía y poder evitar el pago de penalidades y multas por algún tipo de incumplimiento, por otro lado en el plan se tiene considerado todos los recursos necesarios para llevar a cabo la ejecución de dicho plan, de esta manera se evita realizar gastos no planificados por compras de último momento o el pago de personal externo.

La imagen que la compañía ha ido construyendo a lo largo de los años, y el fortalecimiento de la marca en el sector corporativo, ha sido determinante para alcázar la cantidad de clientes que tiene hoy actualmente, por ello es necesario mantener dicha imagen, el contar con un plan de recuperación contribuye con esta labor ya que se puede ejecutar acciones rápidas y efectivas durante un evento crítico, más aún si se logra sobreponerse antes que la competencia genera impacto positivo. Por otro lado, el tener un DRP basado en un estándar internacional genera mayor confianza en los clientes, y puede llegar a ser un factor decisivo al momento de elegir un proveedor.

Otro factor importante a considerar es el tema de la seguridad, en los últimos 2 años se han visto ataques informáticos a nivel global, que han paralizado las operaciones de grandes compañías como es el caso de Telefónica en 2017 (Deloitte, S.L, 2017), el DRP debe ser capaz de cubrir estos escenarios a nivel de seguridad, la norma NIST en la serie 800 tiene un amplio desarrollo en el aspecto de la seguridad que se puede acoplar al DRP tal es el caso de NIST 800-53, que está orientado a los controles de seguridad y privacidad, de esta manera el DRP se puede fortalecer en diversos aspectos y hacerlo más efectivo a fin de garantizar la continuidad de las operaciones.

1.8 Estado del arte

El desarrollo de políticas y estándares relacionados al tema de recuperación ante desastres se ve forzado a tomar una mayor importancia en las organizaciones, luego de acontecimientos históricos que cambian la manera en la que se enfoca la aplicación de la continuidad del negocio.

"Hasta los tristes acontecimientos del 11 de septiembre de 2001 existía cierta conciencia

de la necesidad de establecer planes de recuperación ante desastres, la mayoría de las veces circunscrita a determinados entornos (como el militar, "padre" de la Continuidad, o el sector financiero) y, muy en especial, a sus entornos de tecnologías de la información. Después de este terrible golpe, comienza a percibirse la ineludible necesidad de incluir la Continuidad como un proceso crítico más dentro de la gestión del negocio y que afecta a todas sus áreas."

(Hervias, 2010)

En tal sentido las mejores prácticas de gestión como ITIL, introducen en su proceso la "Gestión de la continuidad de los servicios IT" (IT Service Continuity Management) dentro

de la etapa de diseño de servicio, así mismo COBIT cuenta con el proceso DS4 “Garantizar la Continuidad del Servicio” que se encuentra dentro del dominio entrega y soporte.

1.8.1 Conceptos clave de continuidad de negocio

a) Gestión de la Continuidad del Negocio, BCM (Business Continuity Management)

   Proceso administrativo completo que identifica impactos potenciales que puedan afectar la organización y provee de la estructura para dar flexibilidad y respuestas efectivas para salvaguardar los intereses de los accionistas, la reputación la marca y actividades de valor agregado. (BSI, 2007)

   Responsable: Alta gerencia

   Sistema de gestión de continuidad de negocios, BCMS (Business Continuity Management System)

   La parte del Sistema de Gestión general que establece implementa, opera, monitorea, revisa, mantiene y mejora la continuidad del negocio. (ISO, 2012)

b) El plan de continuidad de negocio (BCP) se puede considerar una metodología interdisciplinaria basada en procedimientos y medidas de seguridad, que ayudan a disminuir la ocurrencia de un desastre, en caso este ocurra, la organización está preparada para afrontar de manera adecuada y rápida, reduciendo el impacto sobre el negocio.

   El plan debe garantizar los aspectos técnicos y organizativos de las áreas críticas. (

c) Plan de Recuperación de Desastres (DRP)

   Es un conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los servicios informáticos críticos en caso de contingencia. (NIST, 2010)

   Focalizado en TI.

d) Plan de Contingencia TI

Es un plan que provee procedimientos y capacidades para proteger y recuperar los principales sistemas de información, aplicaciones o los sistemas de soporte en general.

Focalizado en TI.

No cubre los procesos de negocio

e) Plan de comunicación de crisis:
Es un plan que provee procedimientos para difundir de forma efectiva la ocurrencia de un evento o desastre. (NIST, 2010)

Focalizado en el personal interno y externo

f) Plan de Continuidad de las Operaciones (COOP)
Tiene como objetivo proveer de procedimientos y capacidades para soportar las principales funciones de una organización en un sitio alterno por hasta30 días antes de regresar a las operaciones normales.

Se desarrolla por lo general para la sede principal de una empresa o institución.

No se enfoca en los procesos de TI. (NIST, 2010)

1.8.2 Evolución de normas y estándares

a) Estándar BS25999-1 (código de prácticas)
En noviembre del año 2006 la British Standards Institution (BSI por sus siglas en inglés) publica la norma británica BS25999-1, con la finalidad de proporcionar recomendaciones de códigos de buenas prácticas para una adecuada gestión de continuidad de negocios BCM (business continuity management), para todas las organizaciones, sectores e industrias.

Figura 3 Ciclo de vida de BCM

Fuente: ISACA 2011

El programa de gestión de la continuidad del negocio requiere la definición de una política general, que garantice un adecuado diseño e implementación, dicha política debe definir el alcance, los principios y los recursos dedicados a la gestión de la continuidad, para ello es necesario:

Entender a la organización: el objetivo de esta etapa es identificar procesos, productos y servicios esenciales que forman parte de las actividades críticas de la organización, para lo cual se requiere:

- Identificar los objetivos de la organización y las obligaciones hacia los stakeholders.
- Identificar las actividades, activos y recursos que soportan la entrega de productos y servicios.
- Análisis del impacto en el negocio (BIA): documentar el impacto (económico, reputacional, perdida de información, etc.) de la discontinuidad de los diferentes procesos de negocio, determinando:
    - Periodo máximo de tiempo que los procesos pueden encontrarse inoperativos.
    - Nivel mínimo que los procesos deben alcanzar para ser operativos.
    - Relaciones e interdependencias de los procesos y recursos.
- Identificar y evaluar las potenciales amenazas que podrían causar interrupciones.

Determinar la estrategia del BCM: Esta actividad será determinada por el resultado del tiempo máximo tolerable de interrupción, costos de implementación de estrategias y las consecuencias de no realizar ninguna acción.

Los recursos para esta actividad son los siguientes:

Personas: Establecer estrategia apropiada para cada personal, identificando habilidades, fortalezas y conocimiento clave.

Locales: Establecer estrategias para reducir el impacto de áreas de trabajo, mediante sitios alternativos, trabajo remoto, entre otros.

Tecnología: Establecer estrategias en función a las actividades críticas, para mantener los recursos tecnológicos de respaldo, conectividad, sistemas de continuidad de energía.

Información: Establecer estrategias para para garantizar la confidencialidad, integridad y disponibilidad de la información crítica.

Suministros: Establecer estratégicas para mantener un control de los suministros, manteniendo stocks en almacenes, identificando suministros alternativos y diversificando los proveedores.

Desarrollar e implementar la respuesta BCM: en esta etapa se desarrolla e implementa los planes necesarios para garantizar la continuidad de las actividades críticas y la gestión de incidentes:

Plan de gestión de incidentes: en este plan se debe tener identificado la Lista de tareas y acciones, contactos, actividades del personal, respuesta a los medios de comunicación, gestión de los stakeholders, y formularios para el registro de las actividades durante la incidencia.

Plan de continuidad del negocio: el plan debe contener la lista de tareas y acciones, recursos requeridos, responsabilidades, información de contacto y formularios para el registro de las actividades durante la incidencia.

Plan de recuperación: El plan de recuperación dependerá de las características de la organización y de los incidentes sufridos, siendo uno de los puntos más difíciles de definir con anterioridad.

Probar validar y revisar: La prueba de los planes de incidencias, continuidad y recuperación son necesarios para validar su efectividad, permite desarrollar los conocimientos para afrontar una situación real.

Las pruebas a realizar pueden ser:

Comprobación sobre el papel: Revisar el contenido del BCP

Ensayo: Validar el contenido del BCP a partir de entrevistas.

Simulación: Usar situaciones artificiales para validar que el BCP contiene la información necesaria para una recuperación exitosa.

Prueba de las actividades críticas: Invocar los planes en una situación que no haga peligrar el negocio.

Prueba completa, incluyendo la gestión de incidentes: Prueba real de abandono de edificios, campus, etc.

Será necesario realizar un análisis posterior para identificar aspectos de mejora o puntos desactualizados, acompañado por sistemas de control de versiones y mecanismos para la difusión de los aspectos modificados.

b) BS25999-2 (Especificación)

En el año 2007 se publica la norma BS 25999-2 siendo la primera norma certificable, en el cual se establecen los requisitos para la implementación, auditoría y la certificación de un sistema de gestión de continuidad de negocio. (Bello, 2008)

Los requisitos especificados en la norma BS 25999-2 son genéricos y están destinados a ser aplicables a todas las organizaciones (o partes de ellas), independientemente del tipo, tamaño y naturaleza de la empresa. El grado de aplicación de estos requisitos depende del entorno operativo y la complejidad de la organización.

En esta norma se presenta seis requisitos para que cualquier organización alcance la certificación de continuidad del negocio:

Sección 1. Ámbito de aplicación de la Gestión de continuidad del Negocio. Define el ambiente de aplicación de la norma, así como los requisitos para la implementación de un sistema documentado de la continuidad del negocio.

Sección 2. Términos y Definiciones. Esta sección define los términos y definiciones utilizadas en el cuerpo de la norma.

Esta segunda parte de la BS25999 está basada la estrategia de mejora continua, conocida como el círculo de Demimg “Plan-Do-Check-Act”.

Figura 4 Fases del modelo PDCA

Fuente: ISACA 2011

Sección 3. Planificación de la Continuidad del Sistema de Administración de Empresas (Plan).

Se establece políticas de continuidad negocio, objetivos, controles y procedimientos.

Sección 4. Implementación y funcionamiento de la BCMS (DO) de aplicar en la práctica los planes. Procedimientos para implementar planes de continuidad de negocio

Sección 5. Seguimiento y revisión de la BCMS (Check). Establece las comprobación y control del BCM a partir de auditorías internas, así como la revisión de la Gestión de la Continuidad del Negocio. Así mismo se encarga de monitorear y revisar el performance de las políticas y objetivos

Sección 6. Mantenimiento y Mejora de la BCMS (ACT). Esta sección propone la mejora continua del BCM a través de las acciones preventivas y correctivas del BCM

c) ISO/IEC 24762:2008

Esta norma publicada en el año 2008 por ISO/IEC (International Organization for Standardization) e IEC (International Electrotechnical Commission) da los lineamientos sobre la provisión de los servicios de recuperación ante desastres de tecnología de la información y las comunicaciones (ICT DR por sus siglas en ingles) en el cual se especifica lo siguiente:

- Los requisitos para implementar, operar, monitorear y mantener servicios e instalaciones de la ICT DR.
- Las capacidades que los proveedores de servicios externos deberían poseer y las prácticas que deberían seguir, para proporcionar entornos operativos seguros básicos y facilitar los esfuerzos de recuperación de las organizaciones.
- la guía para la selección del sitio de recuperación, y la guía para los proveedores de servicios de ICT DR para mejorar continuamente sus servicios de ICT DR. (ISO, 2008).

d) BS 25777:2008

En el año 2008 la British Standards Institution (BSI) lanzó la norma BS 25777: 2008 "Gestión de la continuidad de la tecnología de la información y las comunicaciones: código de prácticas", esta norma sirve como ayuda para la planificación y la implementación de estrategias de continuidad de las Tecnologías de la información y la comunicación (TIC) en las organizaciones.

Aquí se desarrolla la relación del concepto de gestión de continuidad de negocio (BCM por sus siglas en ingles) y el concepto de la continuidad de las TIC.

- El concepto de gestión de continuidad del negocio, este concepto se desarrolló a mediados de 1980 como una nueva forma de gestionar los riesgos del negocio, es por ello que la gestión de continuidad de negocio centra en

procesos comerciales completos en lugar de en activos particulares, como los sistemas de TI, porque, para operar una organización debe continuar ejecutando sus procesos comerciales críticos. Estos procesos pueden estar contenidos dentro de una función comercial, o pueden integrar o impactar en varios de ellos. La recuperación de los sistemas de TI por sí sola no mantendrá dichos procesos comerciales en funcionamiento si el personal no tiene las condiciones de trabajo adecuadas, si se han destruido los registros críticos en papel o si la organización no puede comunicarse con sus clientes y proveedores. (ISACA, 2011)

- El concepto de la continuidad de las TIC no solo se centra en la probabilidad y el impacto de los incidentes disruptivos, sino también en la capacidad de la organización para detectar y responder a los incidentes. Esto requiere que las organizaciones monitoreen sus servicios de TIC para asegurar que:
    - Son resistentes y recuperables en el nivel apropiado
    - Cualquier evento inesperado dentro de un servicio se detecta, aborda e investiga de manera oportuna
    - Las dependencias entre los servicios de TIC y los factores externos se conocen y se utilizan para evaluar el riesgo y el impacto de un cambio.
    - Las dependencias de los componentes técnicos son conocidas y utilizadas para evaluar el riesgo y el impacto del cambio.

e) ISO 22301

En el año 2012 se publica la norma ISO 22301:2012 “Seguridad de la sociedad – Sistemas de gestión de la continuidad del negocio - requerimientos” como respuesta a la alta demanda de la norma BS 25999-2, en esta norma se especifica requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado para proteger, reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de incidentes disruptivos cuando surgir.

Los requisitos especificados en ISO 22301:2012 son genéricos y están destinados a ser aplicables a todas las organizaciones, o partes de las mismas, independientemente

del tipo, tamaño y naturaleza de la organización. El grado de aplicación de estos requisitos depende del entorno operativo y la complejidad de la organización.
Sus principales componentes son:

1) Una política.

2) Personas con responsabilidades definidas.

3) Procesos de gestión relacionados con:

- Política
- planificación,
- implementación y operación,
- evaluación del desempeño,
- revisión de la gerencia, y
- mejora

4) Documentación que proporcione evidencia auditable; y cualquier proceso de gestión de continuidad del negocio relevante para la organización.

Según John Sharp (2012) *"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 buenas principios".* (p. 14)

f) NIST SP 800

La serie NIST SP 800, es un conjunto de documentos desarrollados por el Gobierno Federal de EE. UU, en el que se brindan pautas, recomendaciones, informes y especificaciones técnicas que son publicados por el Instituto Nacional de Estándares y Tecnología. Al igual que las series de normas ISO, la serie NIST 800 cuenta con una documentación extensa en temas de seguridad de la información, evaluación de riesgos y planificación de contingencias para los sistemas de información.

NIST SP 800-34 Rev1 (Guía de planificación de contingencias para sistemas de información federales): esta guía fue publicada en el 2002, y actualizada en mayo del 2010 como NIST SP 800-34 Rev1, tiene la finalidad de ayudar a las organizaciones a comprender el propósito, el proceso y el formato del desarrollo de la planificación de contingencias de un sistema de información, en este documento se proporciona información acerca de relación que existe entre planes de contingencia del

sistema de información con otros planes de contingencia relacionados con la gestión de seguridad y emergencias, la resistencia de la organización y el ciclo de vida del desarrollo del sistema. (NIST, 2010)

En la guía se describen los diferentes tipos de planes que existen temas de seguridad y gestión de emergencias:

- Plan de Continuidad de Negocios (BCP por sus siglas en ingles)
- Plan de Continuidad de operaciones (COOP por sus siglas en ingles)
- Plan de Comunicaciones de crisis
- Protección de infraestructura crítica (CIP por sus siglas en ingles)
- Plan de Respuesta a incidentes cibernéticos
- Plan de emergencia del ocupante (OEP por sus siglas en ingles)
- Plan de Recuperación ante desastres (DRP por sus siglas en ingles)
- Plan de contingencia del sistema de información (ISCP por sus siglas en ingles)

1.8.3 Instituciones

BCI (Business Continuity Institute)

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 consisten 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.

BSI (British Standards Institution)

La British Standards Institution se estableció en 1901 como el Comité de Normas de Ingeniería. Posteriormente en 1931 fue adoptada como el nombre de la organización en 1931. BSI tiene un Memorando de Entendimiento con el Gobierno del Reino Unido, que establece la posición de BSI como el reconocido organismo nacional de normas del Reino Unido.

Es una institución independiente sin fines de lucro y ofrece servicios globales en los campos vinculados de estandarización, evaluación de sistemas, certificación de productos, capacitación y servicios de asesoramiento; siendo 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. (ISO, s.f)

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.

DRI International (Disaster Recovery Institute)

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.

NIST (National Institute of Standards and Technology)

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 rev1 (ContingencyPlanning Guide for InformationTechnology Systems) de su serie 800 [NIST, 2010], desarrolla una guía de planes de contingencia de los sistemas de información de cualquier empresa.

1.8.4 Tendencia en los DRP

Recuperación de Desastres como Servicio:

A la variedad de servicios que hoy se pueden brindar con la nube se integra un término denominado Recuperación de desastres como Servicio o DRaaS por sus siglas en inglés, este servicio se basa en la replicación, mediante el alojamiento de información en servidores físicos o virtuales de terceros, tiene como objetivo garantizar la continuidad de las operaciones ante un evento disruptivo, a diferencia de una copia de seguridad almacenada en alguna unidad de almacenamiento, se realiza la réplica en tiempo real ya sea servidores, aplicaciones o bases de datos, esto conlleva a que no es necesario realizar una tarea de restauración de información.

Gartner ha publicado la edición de 2018 de su Cuadrante Mágico para el servicio DRaaS, en el que se ve una diferencia en cuanto al tipo de definición del servicio frente al 2017.

Figura 5 comparación del cuadrante mágico de Gartner entre el año 2017 y 2018

A diferencia del 2017, para la evaluación del informe del 2018 solo se consideraron 10 proveedores, debido al cambio de criterios de evaluación:

Líderes: Iland es el proveedor que se mantiene dentro del cuadrante de líder y se ve una mejoría de su posición con respecto al 2017, por otro lado, Microsoft cambia su posición de visionario a líder.

Visionarios: Los proveedores IBM y Sungard Availability Services cambian su posición de líderes a visionarios con respecto al 2017.

Retadores: El proveedor TierPoint se mantiene en esta categoría, sin embargo, Recovery Point pasa de ser líder a retador con respecto al 2017.

Jugadores de nicho: En categoría fueron incluido los proveedores Bluelock, C&W Business, Expedient y Cloud HPT. (Tecnozero, 2017)

2 MARCO TEORICO

2.1 Conceptos generales

Plan de recuperación Ante desastres DRP

Según NIST un DRP es un plan centrado en el sistema de información, diseñado para restaurar la operatividad del sistema objetivo, la aplicación o la infraestructura de la instalación informática en un sitio alternativo después de una emergencia. El DRP puede estar respaldado por múltiples planes de contingencia del sistema de información para abordar la recuperación de los sistemas individuales afectados una vez que se ha establecido la instalación alternativa. (NIST, 2010)

Evento: Ocurrencia de un conjunto particular de circunstancias (ISO 22301, 3.17)

Incidente: Evento que pudiera constituir o pudiera redundar en una interrupción del negocio, en una pérdida, emergencia o crisis. (ISO 22301, 3.19) Es por ello que se debe tener especial consideración en este tipo de incidentes, como afirma Hotchkiss (2010, p. 26.). "*Eventos de pequeño impacto también pueden causar daño en términos de tiempo de reparación*"

Interrupción: Incidente ya sea previsto o imprevisto que altera el curso normal de las operaciones en una instalación de una organización.

Crisis: Cualquier incidente(s), causado por humanos o causas naturales, que requieren atención urgente y medidas para proteger la vida, lo bienes o el medo ambiente.

Desastre: Situación en la que se han producido amplias pérdidas humanas, materiales, económicas o ambientales que superaron la capacidad de la organización, la comunidad y la sociedad afectadas para responder y recuperarse utilizando sus propios recursos.

Emergencia: Suceso o evento repentino, urgente, generalmente inesperado que requiere acción inmediata. (ISO 22399, 3.6)

Disruptivo: Se puede definir como un evento no planificado que hace que un sistema de información no funcione durante un período de tiempo prolongado. [NIST, 2010]

2.2 Proceso de planificación NIST 800-34

Proceso de planificación de contingencia del sistema de información (NIST 800-34)

La norma NIST 800-34 rev 1, cuenta con siete procesos definidos para desarrollar y mantener un plan de contingencia eficaz del sistema de información:

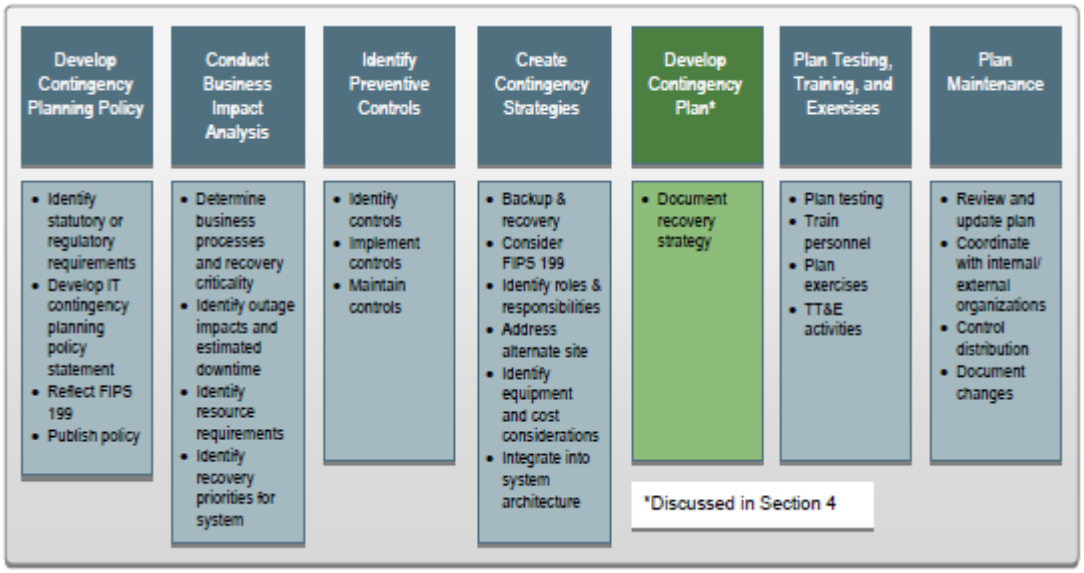


Figura 6 Proceso de planificación de contingencia

Fuente: NIST SP 800-84 Rev.1 2010

2.2.1 Desarrollar la política de planificación de contingencias:

NIST en el capítulo 3.1 de la norma SP 800-34 rev1 señala que para ser eficaz y garantizar que el personal comprenda completamente los requisitos de planificación de contingencia de la organización, el plan de contingencia debe basarse en una política claramente definida. La declaración de política de planificación de contingencia debe definir los objetivos generales de contingencia de la organización y establecer el marco organizacional y las responsabilidades para la planificación de contingencia del sistema. Para tener éxito, la alta gerencia debe apoyar un programa de contingencia e incluirse en el proceso para desarrollar la política del programa. La política debe reflejar los niveles de impacto FIPS 199 y los controles de contingencia que establece cada nivel de impacto. Los elementos clave de la política son los siguientes:

- Roles y responsabilidades
- Alcance del plan de contingencia, funciones y actividades en la organización.
- Requerimiento de recursos

- Requisitos de entrenamiento
- Ejercicios y horarios de prueba
- Plan de mantenimiento programado
- Frecuencia mínima de copias de seguridad y almacenamiento de medios de copia de seguridad.

A medida que los planes de contingencia del sistema de información se desarrollan estas deben coordinarse con las políticas y programas relacionados de toda la organización, incluyendo seguridad del sistema de información, seguridad física, recursos humanos, operaciones del sistema y funciones de preparación para emergencias. Las actividades de contingencia del sistema de información deben ser compatibles con los requisitos del programa para estas áreas, y el personal de recuperación debe coordinarse con los representantes de cada área para mantenerse al tanto de las políticas, programas o capacidades nuevas o en evolución. Los planes de contingencia deben redactarse en coordinación con otros planes asociados con cada sistema objetivo como parte de la estrategia de resiliencia de toda la organización.

El desarrollo de esta fase del proceso de planificación se resume en los siguientes pasos:

- Identificar los requisitos legales o reglamentarios.
- Desarrollar una declaración de política de planificación de contingencia de TI.
- Reflejar FIPS 199 (Normas para la categorización de seguridad de la información federal y los sistemas de información)
- Publicar política

2.2.2 Realizar el análisis de impacto de negocio (BIA)

NIST en su capítulo 3.2 de la norma 800-34 rev1 considera al BIA como un paso clave en la implementación del plan de continuidad y en el proceso de planificación de contingencia en general. El BIA permite al coordinador del Plan de contingencia del sistema de información caracterizar los componentes del sistema, los procesos de misión, negocios compatibles y las interdependencias. El propósito de BIA es correlacionar el sistema con los procesos y servicios críticos y en base a esa información, caracterizar las consecuencias de

una interrupción. El coordinador del Plan de contingencia del sistema de información puede usar los resultados de BIA para determinar los requisitos y prioridades de planificación de contingencia. Los resultados del BIA deben incorporarse adecuadamente en los esfuerzos de desarrollo de análisis y estrategia para el COOP, BCP y DRP de la organización.

Generalmente, hay tres pasos involucrados para lograr el BIA:

- Determinar los procesos de misión / negocio y la importancia de la recuperación. Se identifican los procesos de Misión / Negocios respaldados por el sistema y se determina el impacto de una interrupción del sistema en esos procesos junto con los impactos de interrupción y el tiempo de inactividad estimado. El tiempo de inactividad debe reflejar el tiempo máximo que una organización puede tolerar mientras mantiene la misión.
- Identificar los requisitos de recursos. Los esfuerzos de recuperación realistas requieren una evaluación exhaustiva de los recursos necesarios para reanudar los procesos de misión / negocio y las interdependencias relacionadas lo más rápido posible. Los ejemplos de recursos que deben identificarse incluyen instalaciones, personal, equipo, software, archivos de datos, componentes del sistema y registros vitales.
- Identificar prioridades de recuperación para los recursos del sistema. En función de los resultados de las actividades anteriores, los recursos del sistema pueden vincularse más claramente a la misión crítica / procesos y funciones comerciales. Se pueden establecer niveles de prioridad para secuenciar actividades y recursos de recuperación.

A continuación, se muestra una imagen que resume un sistema de información representativo con múltiples componentes, en que permite enfocar en las actividades del desarrollo del plan, a fin de lograr un plan más efectivo:

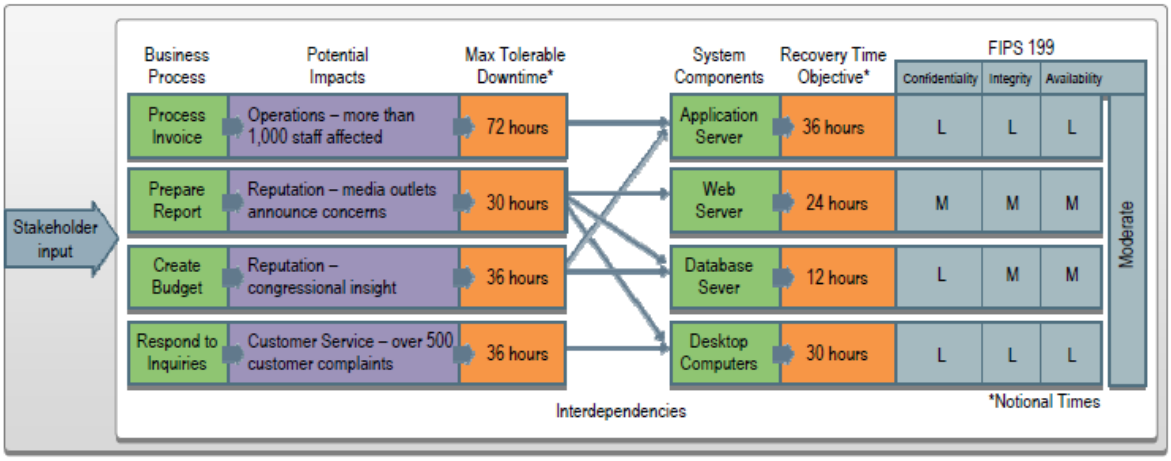


Figura 7 Proceso de análisis de impacto de negocio

Fuente: NIST SP 800-84 Rev.1 2010

2.2.2.1 Determinar procesos de negocio y criticidad de recuperación

NIST en su capítulo 3.2.1 de la norma 800-34 rev1 señala que un sistema de información puede ser muy complejo y, a menudo, admite múltiples procesos de negocios, lo que resulta 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 del plan de contingencia debe trabajar con la gerencia y los puntos de contacto internos y externos para identificar y validar los procesos de negocio. Los impactos de los procesos identificados se analizan luego en términos de disponibilidad, integridad, confidencialidad y el nivel de impacto establecido para el sistema de información.

Los procesos e impactos únicos se pueden expresar en valores o unidades de medida que sean significativos para la organización. Los valores pueden identificarse utilizando una escala y deben caracterizarse como una indicación de la gravedad del impacto para la organización si no se puede realizar el proceso, por ejemplo, se puede crear una categoría de impacto como “Costos” con valores de impacto expresados en términos de personal, horas extras o costos relacionados con los honorarios.

Luego, el Coordinador del plan de contingencia debe analizar los procesos empresariales junto con los propietarios del proceso, el liderazgo y los gerentes comerciales, determinar el tiempo de inactividad aceptable si un proceso determinado o datos específicos del sistema se interrumpieron o no estuvieron disponibles. El tiempo de inactividad se puede identificar de varias maneras.

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

Tiempo objetivo de recuperación (RTO). El RTO define la cantidad máxima de tiempo que un recurso del sistema puede permanecer no disponible antes de que haya un impacto inaceptable en otros recursos del sistema, procesos comerciales y el MTD. Determinar el RTO de recursos del sistema de información es importante para seleccionar las tecnologías apropiadas que sean más adecuadas para cumplir con el MTD. Cuando no es posible cumplir de inmediato con el RTO y el MTD es inflexible, se debe iniciar un Plan de Acción e Hito para documentar el situación y plan para su mitigación.

Punto Objetivo de recuperación (RPO). El RPO representa el punto en el tiempo, antes de una interrupción o una interrupción del sistema, en el que se pueden recuperar los datos del proceso negocio (dada la copia de seguridad más reciente de los datos) después de una interrupción. A diferencia de RTO, RPO no se considera 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 no se exceda el MTD, el RTO normalmente debe ser más corto que el MTD. Por ejemplo, una interrupción del sistema puede evitar que se complete un proceso en particular y, dado que lleva tiempo reprocesar los datos, se debe agregar un tiempo de procesamiento adicional al RTO para permanecer dentro del límite de tiempo establecido por el MTD.

El coordinador del plan de contingencia en coordinación con la administración debe determinar el punto óptimo para recuperar el sistema de información al abordar los factores mencionados anteriormente y al mismo tiempo equilibrar el costo de la inoperancia del

sistema con el costo de los recursos necesarios para restaurar el sistema y su apoyo general para el proceso crítico del negocio.

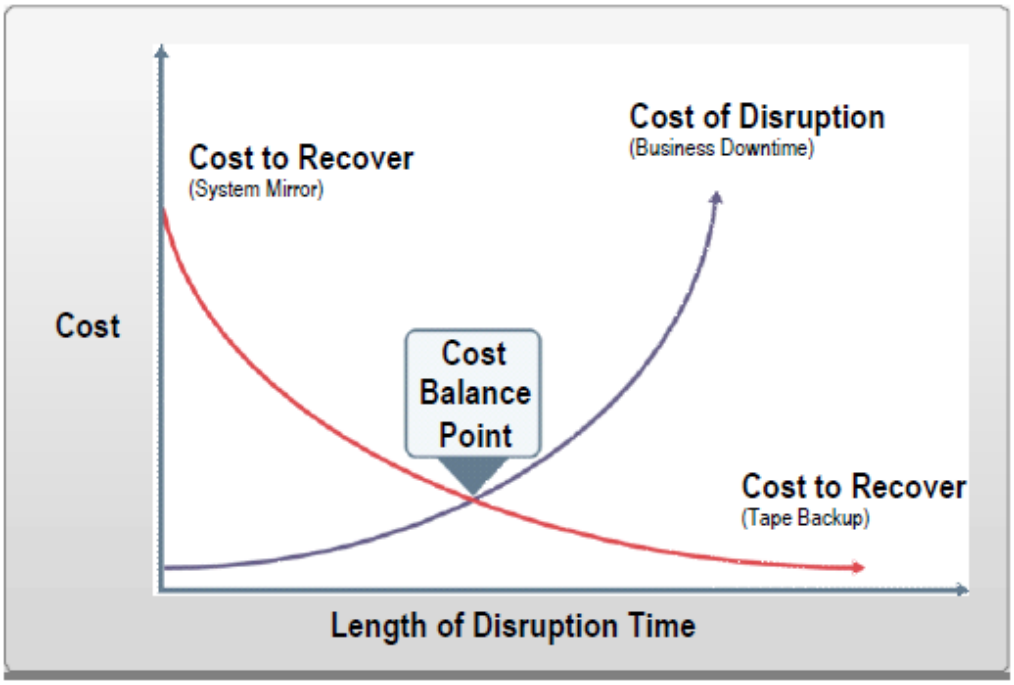


Figura 8 Punto de equilibrio de costo y tiempo de disrupción.

Fuente: NIST SP 800-84 Rev.1 2010

Cuanto más tiempo se permita que continúe una interrupción, más costosa puede ser para la organización y sus operaciones. Por el contrario, cuanto más corto es el RTO, más caras son las soluciones de recuperación que cuesta implementar. Por ejemplo, si el sistema debe recuperarse inmediatamente, las soluciones de tiempo de inactividad cero y los costos alternativos del sitio de procesamiento serán mucho más altos, mientras que un sistema de bajo impacto con un RTO más largo podría implementar un sistema de copia de seguridad en cinta simple menos costoso. Al trazar los puntos de equilibrio de costos se mostrará un punto óptimo entre la interrupción y los costos de recuperación.

El punto de intersección (Punto de equilibrio de costos en la Figura 8: Equilibrio de costos) será diferente para cada organización y sistema en función de las restricciones financieras y los requisitos operativos.

2.2.2.2 Identificar los requisitos de recursos

NIST en su capítulo 3.2.2 de la norma 800-34 rev1 afirma que los esfuerzos de recuperación realistas requieren una evaluación exhaustiva de los recursos necesarios para reanudar los procesos de negocio lo más rápido posible. Al trabajar con la gerencia y los puntos de contactos internos y externos asociados con el sistema, el coordinador del plan de contingencia debe asegurarse de que se identifiquen los recursos completos del sistema de información. Se puede usar una tabla simple como la que se muestra en la Tabla 2 para capturar recursos relevantes del sistema de información.

Tabla 2 Tabla de componentes de recursos

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

Fuente: Plantilla de recursos del sistema de información NIST SP 800-84 Rev.1 2010

2.2.2.3 Identificación de las prioridades de recuperación de recursos del sistema

Desarrollar prioridades de recuperación es el último paso del proceso BIA. Las prioridades de recuperación se pueden establecer de manera efectiva teniendo en cuenta la importancia del proceso crítico del negocio, los impactos del corte, el tiempo de inactividad tolerable y los recursos del sistema. El resultado es una jerarquía de prioridad de recuperación del sistema de información.

Las actividades de esta fase se pueden resumir en:

- Determinar los procesos comerciales y la importancia de la recuperación.
- Identifique los impactos de interrupción y el tiempo de inactividad estimado.
- Identificar los requisitos de recursos.
- Identificar prioridades de recuperación para el sistema.

2.2.3 Identificar controles preventivos

En algunos casos, los impactos de interrupción de servicio identificados en el BIA pueden mitigarse o eliminarse mediante medidas preventivas que disuadan, detecten y/o reduzcan los impactos en el sistema. Donde sea factible y rentable, los métodos preventivos son preferibles a las acciones que pueden ser necesarias para recuperar el sistema después de una interrupción.

El segundo paso incluye la identificación de controles preventivos efectivos para la planificación de contingencias y el mantenimiento de estos controles de manera continua.

Se identifica una variedad de controles preventivos en NIST SP 800-53, según el tipo de sistema y la configuración; Algunas medidas comunes se enumeran a continuación:

- Fuentes de alimentación ininterrumpida (UPS) de tamaño adecuado para proporcionar energía de respaldo a corto plazo a todos los componentes del sistema (incluidos los controles ambientales y de seguridad).
- Generadores a gasolina o diesel para proporcionar energía de respaldo a largo plazo.
- Sistemas de aire acondicionado con exceso de capacidad adecuada para evitar la falla de ciertos componentes, como un compresor.
- Sistemas de extinción de incendios.
- Detectores de fuego y humo.
- Sensores de agua en el techo y el piso de la sala de computadoras.
- Contenedores resistentes al calor e impermeables para medios de respaldo y registros vitales no electrónicos

Las actividades de esta fase se pueden resumir en:

- Identificar controles.
- Implementar controles.
- Mantener controles.

2.2.4 Crear estrategias de contingencia

Se requiere que las organizaciones mitiguen adecuadamente el riesgo derivado del uso de la información y los sistemas de información en la ejecución de los procesos de Negocios. El desafío para las organizaciones es implementar el conjunto correcto de controles de seguridad.

Backup & recovery.:

Los métodos y estrategias de respaldo y recuperación son un medio para restaurar las operaciones del sistema de manera rápida y efectiva después de una interrupción del servicio. Los métodos y estrategias deben abordar los impactos de interrupción y los tiempos de inactividad permitidos identificados en el BIA y deben integrarse en la arquitectura del sistema durante la fase de desarrollo.

Se puede considerar una amplia variedad de enfoques de recuperación, y la elección apropiada depende en gran medida del incidente, el tipo de sistema, el nivel de impacto y los requisitos del sistema:

Se debe tener en consideración el contar con contratos con proveedores alternativos del sitio, acuerdos recíprocos con organizaciones internas y externas y SLAs con proveedores de equipamiento.

Así mismo, al desarrollar una estrategia de recuperación del sistema, se deben considerar tecnologías tales como matrices redundantes de discos independientes (RAID), conmutación por error automática, UPS, agrupación de servidores y sistemas duplicados.

Métodos de respaldo y almacenamiento externo:

El respaldo de los datos del sistema debe ser realizado regularmente, las políticas deben especificar las frecuencias y el alcance de los respaldos, en función de a la criticidad y la frecuencia de los cambios realizados. Las políticas de respaldo de datos deben designar la ubicación de los datos almacenados, las convenciones de nomenclatura de archivos, la frecuencia de rotación de medios y el método para transportar datos fuera del sitio. Se puede hacer una copia de seguridad de los datos en un disco magnético, cinta o discos ópticos, como discos compactos (CD). El método específico elegido para realizar copias de seguridad debe basarse en los requisitos de integridad y disponibilidad del sistema y los datos. Las políticas de respaldo de datos deben designar la ubicación de los datos almacenados, las convenciones de nomenclatura de archivos, la frecuencia de rotación de medios y el método para transportar datos fuera del sitio. Se puede hacer una copia de

seguridad de los datos en un disco magnético, cinta o discos ópticos, como discos compactos (CD). El método específico elegido para realizar copias de seguridad debe basarse en los requisitos de integridad y disponibilidad del sistema y los datos.

Sitios Alternos:

En general, hay tres tipos de sitios alternativos disponibles:

- Sitio dedicado de propiedad u operado por la organización.
- Acuerdo recíproco o memorando de acuerdo con una entidad interna o externa.
- Instalación comercialmente arrendada.

Independientemente del tipo de sitio alternativo elegido, la instalación debe ser capaz de soportar las operaciones del sistema como se define en el plan de contingencia. Los tres tipos de sitios alternativos comúnmente clasificados en términos de su disponibilidad operativa son Cold Sites, Warm Sites o Hot sites.

- Cold Sites: suelen ser instalaciones con espacio e infraestructura adecuados (energía eléctrica, conexiones de telecomunicaciones y controles ambientales) para apoyar las actividades de recuperación del sistema de información.
- Warm Sites: son espacios de oficina parcialmente equipados que contienen parte o la totalidad del hardware del sistema, software, telecomunicaciones y fuentes de energía.
- Hot Sites: son instalaciones de tamaño apropiado para soportar los requisitos del sistema y configurados con el hardware del sistema necesario, la infraestructura de soporte y el personal de soporte.

Adicionalmente a estos tres tipos de sitios alternos existen variaciones y mezclas hibridas, cada organización debe evaluar sus requisitos básicos para establecer la solución más efectiva. Dos ejemplos de variaciones a los tipos de sitio son:

- Mobile Sites: son contenedores autónomos y transportables personalizadas con equipos específicos de telecomunicaciones y sistemas necesarios para cumplir con los requisitos del sistema.
- Mirrored Sites: son instalaciones totalmente redundantes con reflejo de información automatizado en tiempo real. Los sitios duplicados son idénticos al sitio primario en todos los aspectos técnicos.

Consideraciones de costos:

El costo de cada tipo de sitio alternativo, reemplazo de equipo y opción de almacenamiento bajo consideración debe sopesarse frente a las limitaciones presupuestarias. El coordinador debe determinar los gastos conocidos de planificación de contingencias, como los honorarios de contratos alternativos en el sitio, y los que son menos obvios, como el costo de implementar un programa de concientización de contingencia de toda la agencia y el apoyo del contratista. El presupuesto debe ser suficiente para abarcar software, hardware, viajes y envíos, pruebas, planes de programas de capacitación, programas de concientización, horas de trabajo, otros servicios contratados y cualquier otro recurso aplicable (por ejemplo, escritorios, teléfonos, máquinas de fax, bolígrafos y papel). La organización debe realizar un análisis de costo-beneficio para identificar la estrategia de contingencia óptima. La tabla proporciona una plantilla para evaluar las consideraciones de costos.

Roles y responsabilidades:

Después de haber seleccionado e implementado las estrategias de respaldo y recuperación del sistema, se debe designar los equipos apropiados para implementar la estrategia. Cada equipo debe estar capacitado y listo para responder en caso de una situación disruptiva que requiera la activación del plan. El personal de recuperación debe asignarse a uno de varios equipos específicos que responderán al evento, recuperarán capacidades y devolverán el sistema a las operaciones normales. Para hacerlo, los miembros del equipo de recuperación deben comprender claramente el objetivo del esfuerzo de recuperación del equipo, los procedimientos individuales que el equipo ejecutará y cómo las interdependencias entre los equipos de recuperación pueden afectar las estrategias generales.

El tamaño de cada equipo, los títulos de los equipos y los diseños de jerarquía dependen de la organización. Además de un solo rol autorizado para la responsabilidad general de la toma de decisiones, incluida la activación del plan, una estrategia capaz requerirá algunos o todos los siguientes grupos:

- Equipo de gestión
- Equipo de evaluación de interrupciones
- Equipo de administración del sistema operativo

- Equipo de recuperación del servidor (por ejemplo, servidor cliente, servidor web)
- Equipo de recuperación de red de área local / red de área amplia (LAN / WAN)
- Equipo de recuperación de bases de datos
- Equipo de recuperación de operaciones de red
- Equipo (s) de recuperación de aplicaciones
- Equipo de telecomunicaciones
- Equipo de prueba
- Equipo de transporte y reubicación
- Equipo de relaciones con los medios
- Equipo de asuntos legales
- Equipo de seguridad física / personal
- Equipo de adquisiciones (equipos y suministros)

El personal debe ser elegido para formar parte de estos equipos según sus habilidades y conocimientos. Idealmente, los equipos cuentan con personal responsable de las mismas funciones o similares en condiciones normales. Por ejemplo, los miembros del equipo de recuperación del servidor deben incluir los administradores del servidor. Los miembros del equipo deben comprender no solo el propósito del plan de contingencia, sino también los procedimientos necesarios para ejecutar la estrategia de recuperación. Los equipos deben tener un tamaño suficiente para seguir siendo viables si algunos miembros no están disponibles para responder o se pueden designar miembros alternativos del equipo.

2.2.5 Plan de pruebas, entrenamiento y ejercicios TT&E (Plan Testing, Training, and Exercises).

En el capítulo 5.3 la norma NIST 800-34 rev.1 refiere que las organizaciones deben llevar a cabo actividades de TT&E periódicamente, después de los cambios organizacionales o del sistema, o la emisión de una nueva guía de TT&E, o según sea necesario.

La ejecución de eventos de TT&E ayuda a las organizaciones a determinar la efectividad del plan y que todo el personal sepa cuáles son sus roles en la conducción de cada plan del sistema de información.

Pruebas: Las pruebas permiten identificar y abordar las deficiencias del plan al validar uno o más de los componentes del sistema y la operatividad del plan. Las pruebas pueden adoptar

varias formas y cumplir varios objetivos, pero deben realizarse lo más cerca posible de un entorno operativo.

Las siguientes áreas deben abordarse en una prueba de plan de contingencia, según corresponda:

- Procedimientos de notificación
- Recuperación del sistema en una plataforma alternativa desde medios de respaldo
- Conectividad interna y externa
- Rendimiento del sistema con equipos alternativos
- Restauración de operaciones normales

Entrenamiento:
la capacitación al personal con responsabilidades del plan de contingencia debe centrarse en la familiarización de los roles y de las habilidades necesarias para cumplir dichas responsabilidades. Este enfoque ayuda a garantizar que el personal esté preparado para participar en pruebas y ejercicios, así como en eventos de interrupción reales. Se debe proporcionar capacitación al menos una vez anualmente.
El personal debe estar capacitado en la medida en que pueda ejecutar las actividades correspondientes a su rol y responsabilidad sin ayuda de la documentación. Este es un objetivo importante en el caso de que las versiones en papel o electrónicas del plan no estén disponibles durante las primeras horas, como resultado de la interrupción. El personal de recuperación debe estar capacitado en los siguientes elementos del plan:

- Propósito del plan
- Coordinación y comunicación entre equipos
- Procedimientos de reporte
- Requerimientos de seguridad
- Procesos específicos del equipo (fases de activación y notificación, recuperación y reconstitución)
- Responsabilidades individuales (fases de activación y notificación, recuperación y reconstitución)

Ejercicios:

Un ejercicio es una simulación de una emergencia diseñada para validar la viabilidad de uno o más aspectos de un plan de contingencia.

NIST SP 800-84 ha identificado los siguientes tipos de ejercicios que se utilizan en las actividades de TT&E:

- Ejercicios de mesa. Los ejercicios de sobremesa son ejercicios basados en debates en los que el personal se reúne en un aula o en grupos separados para analizar sus roles durante una emergencia y sus respuestas a una situación de emergencia en particular. Un facilitador presenta un escenario y hace a los participantes del ejercicio preguntas relacionadas con el escenario, lo que inicia una discusión entre los participantes sobre los roles, las responsabilidades, la coordinación y la toma de decisiones. Un ejercicio de mesa se basa únicamente en debates y no implica la implementación de equipos u otros recursos.
- Ejercicios Funcionales Los ejercicios funcionales permiten al personal validar su preparación operativa para emergencias al realizar sus tareas en un entorno operativo simulado. Los ejercicios funcionales están diseñados para ejercer los roles y responsabilidades de miembros específicos del equipo, procedimientos y recursos involucrados en uno o más aspectos funcionales de un plan (por ejemplo, comunicaciones, notificaciones de emergencia, configuración del equipo del sistema). Los ejercicios funcionales varían en complejidad y alcance, desde la validación de aspectos específicos de un plan hasta ejercicios a gran escala que abordan todos los elementos del plan. Los ejercicios funcionales permiten al personal ejecutar sus roles y responsabilidades como lo harían en una situación de emergencia real, pero de manera simulada.

2.2.6 Plan de mantenimiento:

Para que sea efectivo, el plan debe mantenerse en un estado listo que refleje con precisión los requisitos del sistema, los procedimientos, la estructura organizativa y las políticas. Durante las diferentes fases de la operación y mantenimiento de los sistemas experimentan cambios frecuentes debido a las necesidades del negocio, actualizaciones tecnológicas, inclusión de nuevas políticas entre otros.

Por lo tanto, es esencial que el plan se revise y actualice regularmente como parte del proceso de gestión de cambios de la organización para garantizar que se documente la nueva información y se revisen las medidas de contingencia si es necesario.

Como regla general, se debe revisar la precisión y la integridad del plan con una frecuencia definida por la organización o cuando se produzcan cambios significativos en cualquier elemento del plan. Ciertos elementos, como las listas de contactos, requerirán revisiones más frecuentes. Los planes para sistemas de impacto moderado o alto deben revisarse con mayor frecuencia. Como mínimo, las revisiones del plan deben centrarse en los siguientes elementos:

- Requerimientos operacionales
- Requerimientos de seguridad
- Procedimientos técnicos
- Hardware, software y otros equipos (tipos, especificaciones y cantidad)
- Nombres e información de contacto de los miembros del equipo
- Nombres e información de contacto de los proveedores, incluidos los POC de proveedores alternativos y externos
- Requisitos de instalaciones alternativas y fuera del sitio
- Registros vitales (electrónicos y en papel).

2.3 Análisis de riesgos

En cuanto al análisis de riesgos se pueden encontrar diferentes definiciones, y metodologías para abordarlo, así mismo se debe considerar la gestión del riesgo como parte importante de los procesos, para ello existen normas internacionales como la ISO 31000. (BSI, 2018)

La norma BS ISO 31000 está enfocada en la gestión de los riesgos proporcionando principios y directivas para apoyar y mejorar las técnicas de tratamiento de riesgos de las compañías.

"*La gestión del riesgo debe contemplar el cálculo del riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia"* (Hiles, 2004)

El enfocar los riesgos a escenario tecnológicos podemos encontrar las siguientes afirmaciones como

"Los sistemas tecnológicos emergentes representan una creciente fuente de nuevos riesgos y vulnerabilidad en la sociedad" (Hellstrom, 2009).

2.3.1 Metodología para el análisis de riesgos

La ISO 27001 plantea una metodología ampliamente usada en materia de seguridad por las industrias para ayudar a identificar los problemas, definir y clasificar su criticidad, para luego realizar algún tipo de acción. (pmg-ssi, 2019)

Esta metodología cuenta con seis fases:

1) Definir el alcance: en esta fase debe delimitar el alcance del trabajo a realizar, para ello es recomendable la participación del directorio y las áreas estratégicas para así considerar dentro del alcance los servicios o procesos.
2) Identificar los activos: una vez definido el alcance, se debe identificar los activos más importantes que estén relacionados con los procesos definidos dentro del alcance, es importante tener actualizado el inventario de activos.
3) Identificar las amenazas: una vez identificados los principales activos, el siguiente paso es identificas las amenazas a las que se encuentran expuesto estos activos, dado que este tema puede ser bastante amplio y diverso, por lo que se requiere un esfuerzo de todo el grupo de trabajo, el cual debe ser multidisciplinario para tener diferentes perspectivas en este aspecto.
4) Identificar vulnerabilidades y salvaguardas: En esta fase se busca analizar las características de los activos, para identificar sus puntos débiles o vulnerabilidades. Una posible vulnerabilidad puede ser identificar un conjunto de servidores cuyos sistemas antivirus no se encuentran actualizados. A la hora de evaluar el riesgo aplicaremos penalizaciones para reflejar las vulnerabilidades identificadas.

   También se debe analizar y documentar las medidas de seguridad implementadas en la compañía.
5) Evaluar el riesgo:

   En esta fase ya se debe contar con los siguientes elementos:

   - Inventario de activos.
   - Conjunto de amenazas a las que está expuesta cada activo
   - Conjunto de vulnerabilidades asociadas a cada activo (si corresponde)
   - Conjunto de medidas de seguridad implantadas

   Con esta información se puede realizar el cálculo del riesgo. Para cada activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el

negocio que esto produciría. El cálculo de riesgo se puede llevar a cabo utilizando tanto criterios cuantitativos como cualitativos.

6) Tratamiento del riesgo:

Los riegos calculados que hayan superado un límite ya establecido se deben elegir estrategias que consisten en:

- Transferir el riesgo a un tercero.
- Eliminar el riesgo.
- Asumir el riesgo, siempre justificadamente.
- Implantar medidas para mitigarlo.

Por su parte NIST 800-30 cuenta con una metodología de evaluación del riesgo de seguridad de la información.

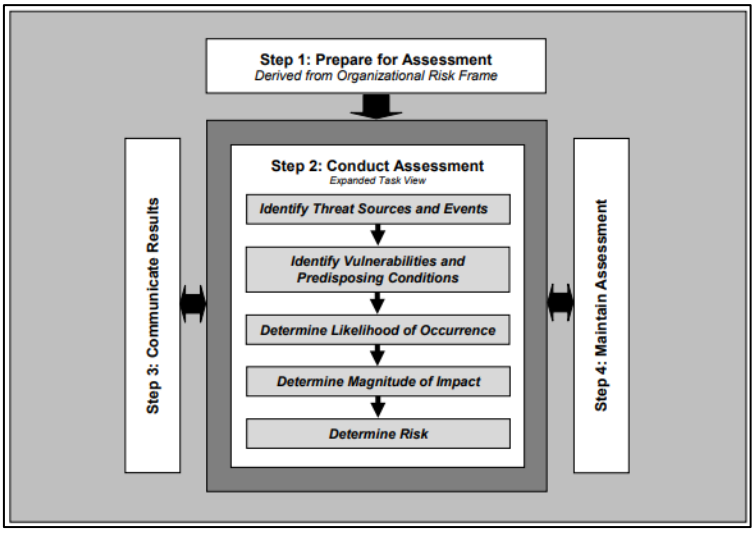


Figura 9 Proceso de análisis de riesgos

Fuente: NIST SP 800-30 rev.1

El proceso está conformado por cuatro pasos:

1) Preparación para la evaluación de riesgos.

El objetivo de este paso es establecer un contexto para la evaluación de riesgos como parte de la preparación y de la gestión de riesgos.

La preparación para una evaluación de riesgos incluye las siguientes tareas:

- Identificar el propósito de la evaluación.
- Identificar el alcance de la evaluación.
- Identificar los supuestos y limitaciones asociados con la evaluación.
- Identificar las fuentes de información que se utilizarán como insumos para la evaluación.
- Identificar el modelo de riesgo y los enfoques analíticos (es decir, enfoques de evaluación y análisis) para ser empleado durante la evaluación.

2) Realizar la evaluación de riesgos

El segundo paso en el proceso de evaluación de riesgos es realizar la evaluación.

El objetivo de este paso es producir una lista de riesgos de seguridad de la información que puede priorizarse por nivel de riesgo y utilizarse para informar las decisiones de respuesta al riesgo. Para lograr este objetivo, las organizaciones analizan las amenazas y vulnerabilidades, los impactos y las probabilidades asociadas con el proceso de evaluación de riesgos.

Este paso también incluye la recopilación de información esencial como parte de cada tarea y se lleva a cabo de acuerdo con el contexto de evaluación establecido en el paso "preparar del proceso de evaluación de riesgos".

La realización de evaluaciones de riesgos incluye las siguientes tareas específicas:

- Identificar las fuentes de amenazas que son relevantes para las organizaciones.
- Identificar eventos de amenaza que podrían ser producidos por esas fuentes.
- Identificar vulnerabilidades dentro de las organizaciones que podrían ser explotadas.
- Determinar la probabilidad de que las fuentes de amenaza identificadas inicien eventos de amenaza específicos.
- Determinar los impactos adversos a las operaciones y recursos de la organización.
- Determinar los riesgos de seguridad de la información como una combinación de probabilidad de explotación de amenazas de vulnerabilidades y el impacto de dicha explotación.

3) Comunicar los resultados de la evaluación

El tercer paso en el proceso de evaluación de riesgos es comunicar los resultados de la evaluación y compartir información relacionada con los riesgos. El objetivo de este paso es garantizar que los responsables de la toma de decisiones en toda la organización tengan la información relacionada con el riesgo necesaria para informar y guiar las decisiones de riesgo. La comunicación y el intercambio de información consta de las siguientes tareas específicas:

- Comunicar los resultados de la evaluación de riesgos; y
- Compartir información desarrollada en la ejecución de la evaluación de riesgos, para respaldar otros riesgos.

4) Mantener la evaluación

El cuarto paso en el proceso de evaluación de riesgos es mantener la evaluación. El objetivo de este paso es mantener actualizado el conocimiento específico de las organizaciones de riesgo. (NIST, 2012)

3 DEFINICIÓN DEL PROBLLEMA

3.1 Análisis del problema

Como se mencionó en el capítulo 1.3, la principal problemática es que no se cuenta con un plan que garantice la continuidad de las operaciones de la compañía ante un evento disruptivo ocasionado por diversos factores relacionados a la falta de documentación, pruebas sistemas de respaldo, entre otros, por tal motivo se han identificado situaciones problemáticas específicas que evidencian lo mencionado en el capítulo 1.3 y como podría impactar a la compañía en un escenario de desastre.

Los problemas identificados en la organización son:

Dependencia de personal único especializado, hace que el conocimiento de los procesos críticos que son soportados por la red backbone se concentre en pocas personas, durante una avería de alto impacto se requiere contactar a este personal, lo cual puede llegar a presentar un problema en caso la disponibilidad de dicho personal no sea inmediata, en consecuencia puede llegar a impactar en los SLA, por tal motivo existe la necesidad de organizar un esquema de personal suplente que pueda asumir el rol en caso este no se encuentre disponible, a continuación se describen los roles del personal especializado que no cuenta con un suplente.

Tabla 3 Listado de personal especializado y sus funciones

Cargo	Área
Especialista senior de redes (CCIE)	CORE
Especialista de seguridad Fortinet.	CORE
Especialista de optimización de redes. (CCIE)	NOC
Especialista senior de seguridad.	CIBERSOC

- Falta de documentación de manuales, procedimientos, inventarios y diagramas puede generar inconvenientes al momento de afrontar algún evento disruptivo, ya que al no contar con una información o el contar con alguna información no actualizada y poco confiable puede llevar a cometer algún error involuntario o retrasos en la ejecución de trabajos de recuperación impactando directamente en los SLA, otra de las necesidades de contar con esta información actualizada facilita la transferencia de conocimientos.

A continuación, se han reunido un listado de la documentación actual con la que se cuenta y la que se sugiere tener:

Tabla 4 Documentación de procedimientos

Documentación	Estado
Procedimiento de recuperación de servicios de Internet	Desactualizado
Procedimiento de recuperación de servicios de Servicios gestionados	Desactualizado
Procedimiento de recuperación de servicios de L2L	Desactualizado
Procedimiento de instalación de tarjetas y módulos	Desactualizado
Procedimiento de conmutación de proveedores de internet	Desactualizado
Procedimiento de cambio de supervisoras	no se cuenta
Procedimiento de mitigación con herramienta anti DDoS	Actualizado
Procedimiento de mitigación con herramienta blackhole	no se cuenta
Procedimiento de recuperación de nodos	no se cuenta
Procedimiento de atención de tickets de avería	no se cuenta
Lista de contactos y escalamiento	Actualizado
Diagrama de red backbone	Actualizado
Inventarios de red	Actualizado
Inventarios de direccionamiento IP privado	Actualizado
Inventarios de direccionamiento IP Publico	Actualizado
Inventarios de direccionamiento IPv6	Actualizado
Manual de instalación de equipos marca Cisco	no se cuenta
Manual de instalación de equipos marca Huawei	no se cuenta
Manuales de configuración de servicios MPLS	Actualizado
Manual de configuración y troubleshooting de QoS	Desactualizado

- Falta de Protocolos o estrategias establecidos para actuar en determinados escenarios, como incendios, inundaciones, terremotos, entro otros casos puede llegar a generar un impacto en los procesos de negocio, imagen, prestigio o incluso en la seguridad y la integridad de las personas, al no tener definidos los sitios de respaldo donde continuar con las operaciones más críticas o incluso no contar con un comité de crisis que pueda responder rápidamente a las necesidades del negocio hacen difícil que la organización pueda afrontar de manera exitosa un evento disruptivo.

Tabla 5 Listado de protocolos ausentes

Protocolos	Estado
Protocolo para escenario de incendio.	no se cuenta
Protocolo para escenario de inundación.	no se cuenta
Protocolo para escenario de terremoto.	no se cuenta

Protocolo para escenario de corte de energía eléctrica prolongado.	no se cuenta
Protocolo para escenario de ataques informáticos.	no se cuenta
Protocolo para escenario de falta de personal especializado.	no se cuenta

- Ataques informáticos de tipo DDoS, están ocurriendo de manera muy frecuente en todas partes del mundo de manera diaria, como se muestra en la siguiente imagen correspondiente a los ataques más significativos de las últimas 24 horas registradas por el portal ATLAS de Arbor Networks.

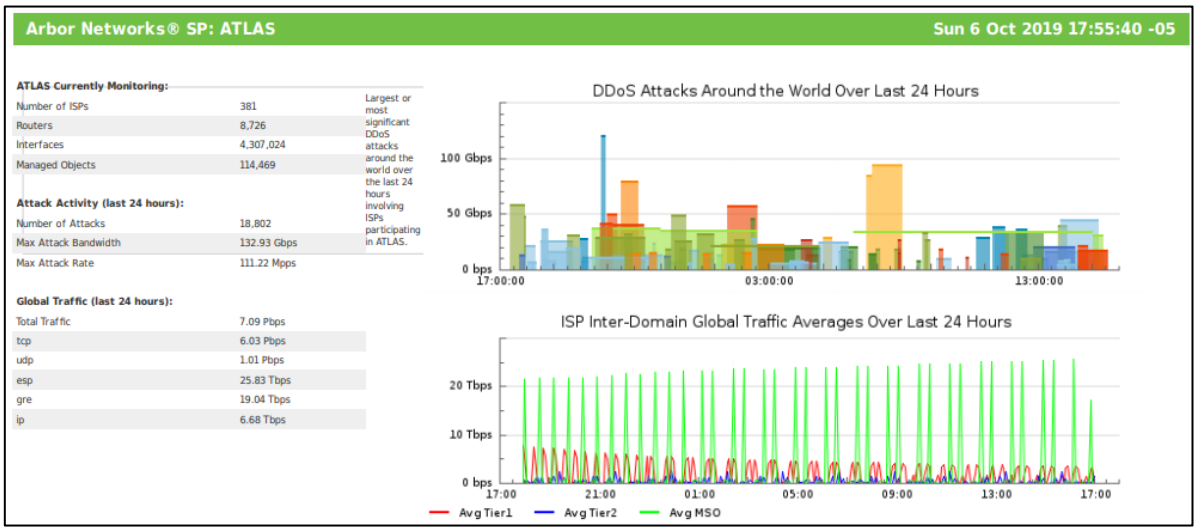


Figura 10 Reporte de ataques de tipo DDoS de 24 horas

Fuente: Herramienta interna, Atlas Arbor Networks

En este reporte podemos observar que se han producido 18,802 ataques en 381 proveedores de servicio a nivel mundial en tan solo 24 horas con un impacto máximo de 132.93 Gbps. En este contexto podemos decir que estos ataques informáticos no son ajenos a la compañía ya que eventualmente ocurren ataques DDoS que superan los 40 Gbps generando inestabilidades del servicio, en la siguiente imagen se puede apreciar uno de los correos emitidos de manera interna donde se aprecia un ataque volumétrico de 48.2 Gbps haciendo uso del protocolo UDP (LDAP) y Fragmentación de IP por un periodo de 10 minutos.

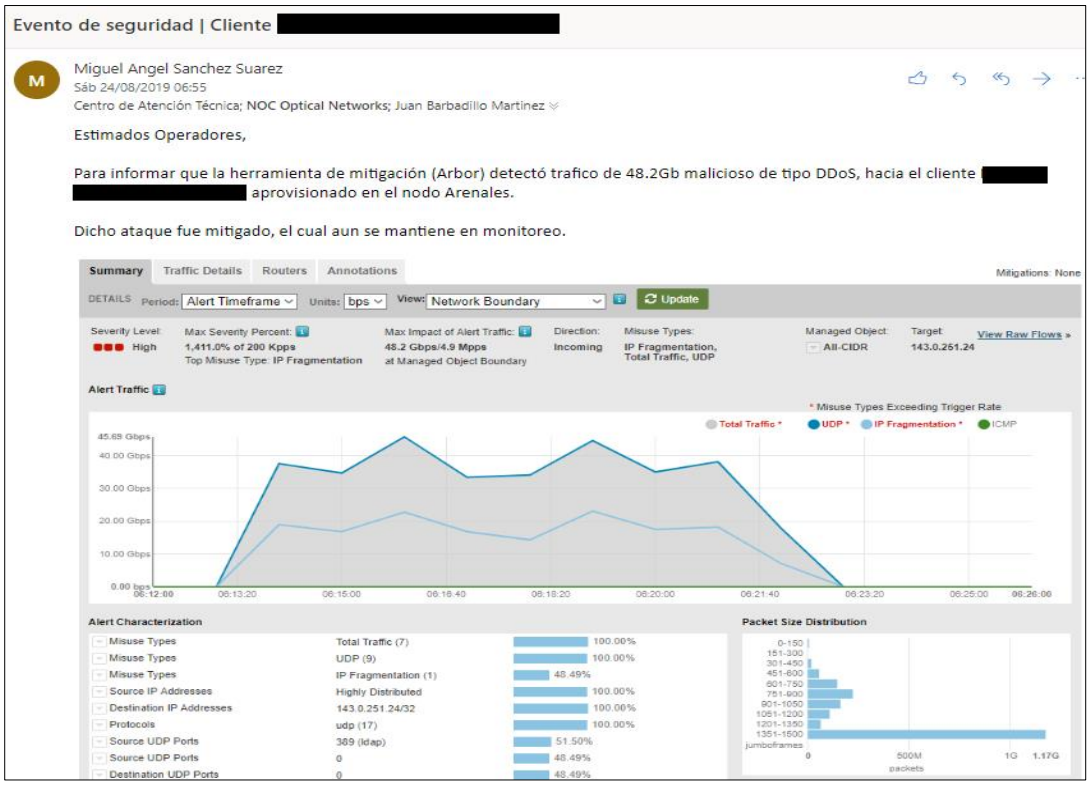


Figura 11 Evidencia de ataques DDoS a la compañía.
Fuente: Correo interno de la compañía.

- Afectación en la planta externa, en una de las causas más comunes en cuanto a las interrupciones de servicios se refiere, al tener una planta externa de más de 4500 km de fibra óptica se es susceptible a las constantes averías ya sea por trabajos municipales, accidentes de tránsito, robo de materiales, manipulaciones por terceros o actos vandálicos entre otros, todas estas causas representan el 47.32% del total de las averías que han generado una interrupción en la compañía en el primer semestre del año 2019 según se indica en la tabla 3.
- Las fallas ocasionadas por el proveedor representan el 18.75% de las averías debido a que la empresa requiere de proveedores de transporte de datos para llegar a las provincias, por otro lado, los proveedores que dan la salida internacional no están libres de fallos en su red por lo que es otro de los factores a considerar para elaborar el DRP.
- Las fallas lógicas ocasionaron un 16.07% de las interrupciones en el primer semestre del 2019, esto ocasionado por comportamientos anómalos de equipos que han presentado fallas por obsolescencia o algún bug de que ha ocasionado un comportamiento inesperado desencadenando una afectación del servicio.

Tabla 6 Reporte de averías por categorías en el primer semestre del año 2019

Reporte de interno de averías de la compañía entre los meses de enero hasta julio 2019 emitido por el área NOC.

Tabla de distribución por Categoría

Categoría	Cant	%	Tempo(min)	Tiempo %
Medio_Físico	53	47.32%	277036	61.71%
Proveedor	21	18.75%	98554	21.95%
Lógico	18	16.07%	49682	11.07%
Hardware	4	3.57%	8170	1.82%
Configuración	1	0.89%	7308	1.63%
Eléctrico	14	12.50%	5507	1.23%
Operador	1	0.89%	2640	0.59%
Total, general	**112**	**100.00%**	**448897**	**100.00%**

Fuente: Informe interno de la compañía.

- Falta de un plan de pruebas; si bien es cierto que existen sistema de respaldo entre diferentes sedes, sistemas de alta disponibilidad a nivel de equipamiento, enlaces de contingencia en cuanto a proveedores, no se ha realizado pruebas o simulacros que garantice el correcto funcionamiento de estos sistemas de respaldo durante la ocurrencia de un evento disruptivo, por tal motivo es necesario establecer cronogramas y ejecutarlas, a fin de identificar fallas de algún elemento y poder proponer acciones de mejora.

3.2 Interesados

En la siguiente matriz se ha identificado a los interesados del proyecto de diseño de un plan de recuperación ante desastres.

Tabla 7 Tabla de interesados

Nombre de interesado	Posición / titulo	Rol	Expectativas	Influencias	Interés	Estrategia para recibir apoyo o reducir obstáculos
Usuarios de internet, interconexi	Cliente	Cliente (recibe el	Acceder a los servicios de internet y	Media	Alto	Todos los trabajos de instalación, cambios

ón de datos y Seguridad de Gestionada.		servicio final)	transmisión de datos de forma rápida y segura, contando con la disponibilidad del servicio las 24 horas los 365 días al año			o pruebas durante la realización del proyecto DRP que implique una afectación de los servicios debe ser comunicado con antelación a los clientes. Conseguir un feedback de los clientes después de realizado las pruebas.
Presidente de directorio	Director	Presidente de directorio	El DRP debe eficiente y ser capaz de reanudar las operaciones en el menor tiempo posible una vez ocurrido el desastre.	Alta	Alto	Mantener informados del desarrollo del Proyecto.
Gerencia de redes y servicios	Gerente	Gerente	El DRP debe eficiente y ser capaz de reanudar las operaciones en el menor tiempo posible una vez ocurrido el desastre.	Alta	Alto	Mantener informados del desarrollo del Proyecto.
Jefe de proyecto	Project Manager	Project Manager	La ejecución del proyecto sea realizado de acuerdo con los planteamientos realizados.	Alta	Alto	Comunicación constante durante el desarrollo del proyecto
Proveedores	Comercial	Proveedor	Cumplir con los contratos y acuerdos establecidos.	Media	Medio	Comunicación constante durante el desarrollo del proyecto
Área Financiera	Área de finanzas	Jefe de finanzas	Manejo adecuado de las cuentas financiera durante el proyecto, créditos, avales, etc.	Alta	bajo	Comunicación constante durante el desarrollo del proyecto
Áreas de Ingeniería / NOC (Network Operation Center)	Áreas de Ingeniería	Áreas de Ingeniería	El proyecto permita el funcionamiento óptimo de los servicios que las áreas administran.	Alta	Alto	Comunicación constante durante el desarrollo del proyecto

Area del TAC (Technical Assistance Center)	TAC	TAC	Que la ejecución del proyecto sea según lo planificado, para que puedan informar y recopilar los problemas que el cliente final pueda tener.	Media	Medio	Comunicación constante con el cliente final.

Fuente: elaboración propia.

Los requerimientos que se plantean para el diseño del plan de recuperación ante desastres deben de cumplir los objetivos específicos planteados en el capítulo 1.5.2, por tal motivo en el desarrollo del proyecto se debe cumplir con cada uno de los requerimientos que se mencionan a continuación:

Tabla 8 Requerimientos alineados a los objetivos específicos

Objetivo Especifico	Requerimientos
Identificar los procesos críticos de la compañía que permita calcular el impacto operacional y financiero, para su priorización ante un desastre.	Se debe Identificar los procesos críticos de la compañía y evaluar el tipo de impacto.
	Se debe determinar el impacto financiero estimado por cada uno de los procesos identificados.
	Se debe calcular los valores para: MTD (Tiempo de Inactividad Máximo Tolerable) RTO (Tiempo Objetivo de Recuperación) RPO (Punto Objetivo de Recuperación)
	Se debe documentar el BIA con todos los requerimientos anteriores.
Identificar los escenarios y los riesgos críticos que puedan impactar el normal funcionamiento de los procesos críticos del negocio.	Se debe realizar un inventario de todos los recursos que soportan los procesos críticos de la compañía y establecer su nivel de criticidad.
	Se debe identificar los riesgos de los recursos que soportan los procesos críticos y establecer su probabilidad de ocurrencia y el nivel de impacto sobre los servicios críticos de la compañía.
	Se debe realizar un tratamiento de los riesgos que se encuentren en la categoría de riesgo intolerable.

	Se debe identificar los escenarios que puedan afectar a los procesos críticos de negocio y definir sus impactos potenciales.
Desarrollar estrategias y procedimientos de recuperación para los escenarios definidos.	Se debe identificar los recursos necesarios para cada uno de los escenarios identificados.
	Se debe desarrollar una o más estrategias por cada uno de los escenarios identificados.
	Se debe desarrollar procedimientos por cada uno de los escenarios identificados.
	Se debe definir los roles y responsabilidades por cada una de las estrategias.
Requerimientos del proyecto.	Se debe realizar un plan de pruebas para los escenarios definidos.
	Se debe evidenciar las pruebas realizadas mediante, correos, fotos, gráficos de herramientas.

Fuente: Elaboración propia

3.3 EDT

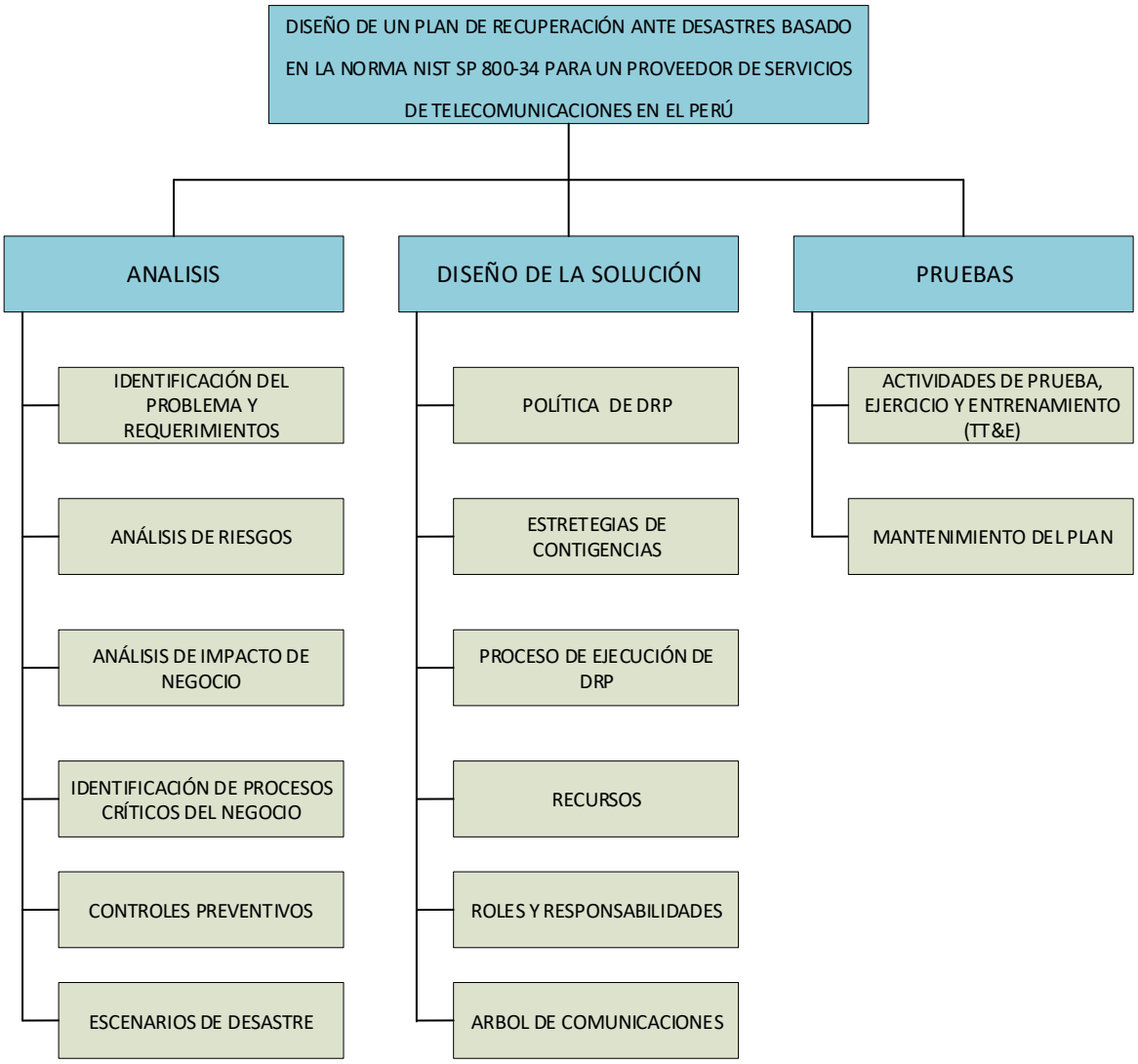


Figura 12 EDT
Fuente: elaboración propia

4 DISEÑO DE LA SOLUCIÓN

En este capítulo se desarrollará el diseño del plan de recuperación ante desastres, haciendo uso de las recomendaciones de la norma NIST 800-34 y cumpliendo los procesos de planificación de contingencia del sistema de información a fin de cumplir con los objetivos y los requerimientos planteados.

4.1 Política de plan de recuperación ante desastres

a) Objetivos

El objetivo de plan de recuperación ante desastres es asegurar que la empresa esté preparada para responder a eventos catalogados como desastres y/o emergencias, cuya consecuencia sea la interrupción de las operaciones normales, y permita recuperarse en el menor tiempo posible con un nivel de servicio aceptable para los clientes.

b) Alcance

El alcance de la Política aplica a los principales procesos de negocio de la empresa que permite proveer el Servicio de Internet, Interconexión de Sedes y Servicios Gestionados. Se han considerado varias situaciones de desastre. Para cada uno de los escenarios se han definido los eventos que los desencadenarían, acciones a realizar en caso de desastres y vuelta a la normalidad de las operaciones.

c) Referencia

- Norma NIST 800-34 rev1

d) Vigencia

Lo dispuesto en la presente política es de uso obligatorio, entrará en vigor a partir de la fecha de su aprobación y permanecerá vigente hasta la aprobación y publicación de otro documento de similar jerarquía que lo sustituya.

e) Comunicación de la política

Se debe asegurar que la política sea comunicada, entendida e implementada en toda la organización y sea de conocimiento de los colaboradores y demás partes interesadas, conservándose evidencia de su recepción y aceptación.

f) Mejora continua

La Política del plan de recuperación ante desastres deberá ser revisada por lo menos una vez al año o si ocurren cambios significativos para garantizar su idoneidad, adecuación y efectividad continua.

g) Compromisos

La Alta Dirección de la empresa reconoce que el plan de recuperación ante desastres es un objetivo primordial para el desarrollo del negocio, el mismo que debe ser impulsado y apoyado por todos los miembros de la organización.

Esto incluye los siguientes compromisos:

- Cumplir con los objetivos del plan de recuperación ante desastres.
- Cumplir con los requisitos planteados para el desarrollo del plan.
- Asignar los recursos humanos y financieros necesarios para el desarrollo e implementación del plan.
- Comunicar el alcance, los planes, las políticas y los objetivos.
- Asegurarse de que se lleve a cabo los ejercicios de DRP según los cronogramas establecidos.
- Mejorar continuamente el plan de recuperación ante desastres.

h) Responsabilidades

- Responsabilidades de las gerencias:
  - Los responsables de los procesos de negocio deben planificar, en coordinación con el responsable del plan de recuperación ante desastres, los recursos que requieran para el desarrollo de las estrategias de continuidad a incorporar en sus respectivos planes, los que deberán incluirse en los presupuestos anuales.
  - Realizar y participar en las actividades y acciones que permitan mantener el plan de recuperación ante desastres vigente y con los controles adecuados.
- Responsabilidades de los colaboradores:
  - Comunicar cualquier acción, evento o escenario que pueda desencadenar en una crisis para la continuidad de las operaciones de la empresa.
  - Participar en los equipos de trabajo, actividades y acciones relacionadas al plan de recuperación ante desastres.
  - Conocer y cumplir con lo establecido en el plan de recuperación ante desastres aprobadas y vigentes.

i) Formación y capacitación

Para garantizar el correcto y eficiente funcionamiento del DRP y asegurar la competencia de las personas que en él intervienen, se realizarán las acciones de formación, concientización y comunicación acorde con las necesidades de la empresa.

Entre estas capacitaciones a realizar se deberán incluir:

- Capacitaciones sobre las necesidades de gestión y técnicas del plan de recuperación ante desastres.
- Concientización sobre la documentación presente en el plan de recuperación ante desastres y su importancia.
- Capacitaciones requeridas para cumplir con los requisitos del plan de recuperación ante desastres.

j) Pruebas de DRP

La realización de pruebas de recuperación ante desastres planificados permite que todos los miembros de los equipos de DRP estén familiarizados con los planes, lo cual mejora la eficacia de los mismos.

- Se debe establecer un cronograma de pruebas anual para los escenarios de desastres identificados, a fin de probar la eficacia de las actividades de recuperación técnica, disponibilidad de sitios alternos, respuesta de recursos y servicios de proveedores.
- En cada prueba se deben fijar los objetivos de la prueba, alcance, resultados esperados, recursos, indicadores de desempeño y el informe de resultados en el cual se incluirán las observaciones y/o recomendaciones de la respuesta de las estrategias seleccionadas para el escenario de contingencia probado.
- El personal que las realice deberá ser debidamente formado antes de su realización.
- La realización de pruebas no debe poner en riesgo la operación normal de los servicios.
- Las pruebas al plan quedarán documentadas y deberán realizarse al menos una vez al año.
- Se debe considerar la prueba integral del Plan, mediante una única prueba o una secuencia de ellas, por lo menos una vez al año para asegurar la efectividad del mismo.

k) Revisión de la política

Se desbeberá garantizar la revisión de la política al menos una vez al año y todos los cambios deberán ser registrados en el control de cambios.

4.2 Análisis de impacto de negocio BIA

a) Objetivo

El objetivo del Análisis de Impacto en el Negocio es determinar y entender qué servicios son esenciales para la continuidad de las operaciones y calcular su posible impacto.

b) Alcance

El Alcance del Análisis de Impacto en el Negocio comprende específicamente la operación de los Servicios:

- Internet: Servicio de acceso dedicado a internet con un overbooking[6] de 1:1, con conexión directa al NAP Perú.
- Interconexión de sedes: Servicio que permite interconectar sedes mediante redes de capa 2 y capa 3 entre una o más vlans.

c) Servicios gestionados: Servicio que permite ofrecer la gestión de diferentes servicios, incluidos enlaces, seguridad, cámaras, etc.

d) Fases del BIA

Para el desarrollo del BIA se han definido las siguientes fases:

Tabla 9 Fases del BIA

ACTIVIDAD	DESCRIPCION
1	Identificar los procesos críticos y evaluar el tipo de impacto.
2	Determinar el Impacto Financiero estimado
3	Determinar del MTD (Tiempo de inactividad máximo tolerable).
4	Determinación del RTO (Tiempo Objetivo de Recuperación).
5	Determinación del RPO (Punto Objetivo de Recuperación).
6	Identificación de los recursos que soportan los procesos de negocio.

[6] Método utilizado en telecomunicaciones para maximizar el uso de las líneas físicas, relacionado a la reserva de ancho de banda. (Ball, 2004)

Tabla 10 Procesos críticos y servicios

Procesos de negocio	Códigos	servicios
Internet	INT	Internet dedicado para empresas
		Internet con HA
		Internet seguro
		Internet seguro avanzado
Interconexión de sedes	L2L	Lan to Lan
		Lan extendida
		Ultima milla
		Fibra oscura
Servicios gestionados	S.G	SG de enlaces
		SG de cámaras
		SG de seguridad
		SG de Lan
		SG de WIFI
Telefonía	TELF	SIP trunk
		Centrales virtuales
		Colaboración y videoconferencia
Servicios en la nube	S.N	Infraestructura y plataforma
		Colaboración y productividad
Servicios adicionales	S.A	Gestión compartida
		Monitor
Co-ubicación	CO-U	Co-ubicación
Lan center	LC	Lan center
		go-games
Streaming	ST	Streaming

En la tabla 10 se lista los procesos de negocio que soportan a la compañía, cada uno de estos procesos de negocio cuenta con una estructura propia de modelo de negocio, flujos y procesos que hacen que los servicios puedan ser ofrecidos.

Tabla 11 Procesos de negocio y Tipo de impactos

N°	Procesos de negocio	Tipo de Impacto (Alto, Medio, Bajo)				
		Financiero	Reputación	Legal y Regulatorio	Contractual	Objetivos del Negocio
		Pérdidas financieras debido a multas, sanciones, pérdida de beneficios o disminuyen la cuota de Mercado.	Opinión negativa o daños a la imagen)	Litigios, suspensión o retiro de licencias para el comercio.	Incumplimiento de contratos y obligaciones entre las organizaciones.	Si no se cumplen los objetivos fijados o se ven afectados.
1	Internet	Alto	Alto	Alto	Alto	Alto
2	Interconexión de sedes.	Medio	Alto	Alto	MEDIO	MEDIO
3	Servicios gestionados	Medio	Medio	Medio	Medio	Medio
4	Telefonía	Bajo	Bajo	Bajo	Bajo	Bajo
5	Servicios en la nube	Bajo	Bajo	Bajo	Bajo	Bajo
6	Servicios adicionales	Bajo	Bajo	Bajo	Bajo	Bajo
7	Co-ubicación	Bajo	Bajo	Bajo	Bajo	Bajo
8	Lan center	Bajo	Bajo	Bajo	Bajo	Bajo
9	Streaming	Bajo	Bajo	Bajo	Bajo	Bajo

Tabla 12 Leyenda análisis de BIA

Impacto	Descripción
ALTO	• Su costo de interrupción genera a nivel a financiero un impacto significativo debido a multas y sanciones. • Ocasiona pérdida de ingresos. • Genera daño a la Reputación. • Conlleva a la pérdida del cliente.
MEDIO	• Su ausencia afecta parcialmente a un proceso crítico de la empresa • Costos de interrupción medio. • Generen reclamo sin costo.
BAJO	• Su ausencia no afecta a ningún proceso crítico de la empresa. • Costos de interrupción bajo. • No generen reclamos ni penalidades.

Impacto Financiero

Se debe estimar las pérdidas económicas para la organización por la falta del servicio.

El criterio para determinar las pérdidas económicas es en base la facturación anual y al porcentaje que significan para el negocio.

Para lo cual se utiliza el cuadro de referencia siguiente:

Tabla 13 Porcentaje de facturación anual por proceso de negocio

Servicio	Porcentaje de la facturación anual
Internet	45%
Interconexión de sedes	30%
Servicios gestionados	15%
Otros	10%
TOTAL	100%

Una vez determinado el porcentaje, los resultados del Impacto Financiero se calculan en base a la facturación anual y el porcentaje de cada servicio dividido en horas:

Tabla 14 Pérdidas económicas de cada proceso de negocio por hora

N°	Servicio	Pérdidas Económicas Por Hora
1	Internet	S/ 199 325.39
2	Interconexión de sedes	S/ 153 374.72
3	Servicios gestionados	S/ 12 801.01

Determinación del RPO

Tabla 15 Valor de RPO por cada proceso de negocio.

N°	Servicio	Tolerancia Máxima de perdida de datos (RPO)
1	Internet	2 horas
2	Interconexión de sedes	3 horas
3	Servicios gestionados	3 horas
4	Otros	6 horas

Determinación del RTO:

Es el periodo inmediatamente posterior a la ocurrencia de un incidente dentro del cual deben reanudarse la prestación de servicios, o la reanudación de actividades, o la recuperación de recursos. Este tiempo debe ocurrir antes del MTD.

Tabla 16 Valor de RTO para cada proceso de negocio

N.º	Servicio	Tiempo de Recuperación Objetivo (RTO)						
		< 5 Minutos	< 15 Minutos	< 30 Minutos	< 1 Hora	< 2 Horas.	< 5 Horas.	Tiempo Específico
1	Internet	-	-	-	-	-	-	02 horas
2	Interconexión de sedes	-	-	-	-	-	-	03 horas
3	Servicios gestionados	-	-	-	-	-	-	03 horas

Determinación del WRT

Tiempo requerido para recuperar la información perdida (Basado en el RPO), así como de ingresar al sistema todos los datos que se generaron durante la caída del sistema.

Tabla 17 Valor de WRT para cada proceso de negocio

N.º	Servicio	Work Recovery Time (WRT)							
		< 5 Minutos	< 15 Minutos	< 30 Minutos	< 1 Hora	< 2 Horas.	< 5 Horas.	< 12 Horas	Tiempo Específico
1	Internet	-	-	-	-	-	-	-	01 horas
2	Interconexión de sedes	-	-	-	-	-	-	-	02 horas
3	Servicios gestionados	-	-	-	-	-	-	-	02 horas

Determinación del MTD

Tabla 18 Factores para el cálculo de MTD por proceso de negocio

Factores para toma de decisión del MTD	Internet	L2L	S.G
	Tiempo en minutos		
Tiempo de detección de falla	2	2	2
Tiempo de diagnostico	10	10	10
Toma de decisión	10	10	10
Ejecutar procedimiento desde el centro de operaciones	20	60	60
Comunicación con proveedores	28	28	28
Equipos y materiales	20	20	20
Traslado de equipo de respuesta	30	30	30
Ejecutar procedimiento en sitio (wrt)	60	80	80
Otros factores no contemplados	60	120	120
	240	360	360

Estos factores para el cálculo del WRT fueron en base a experiencias anteriores y a la metodología juicio de expertos.

Determinación del MTD:

Tiempo máximo que un servicio puede ser interrumpido sin causar un daño significativo a la misión de la organización:

Tabla 19 Valores para el MTD por proceso de negocio.

N.º	Servicio	Tiempo de inactividad máximo tolerable (MTD)								
		< 5 Minutos	< 15 Minutos	< 30 Minutos	< 1 Hora	< 2 Horas.	< 5 Horas.	< 12 Horas	Tiempo Específico	Prioridades de recuperación
1	Internet	-	-	-	-	-	-	-	04 horas	Alta
2	Interconexión de sedes	-	-	-	-	-	-	-	06 horas	Alta
3	Servicios gestionados	-	-	-	-	-	-	-	06 horas	Media

Recursos Críticos y Prioridades:

Se deben identificar para cada servicio los recursos críticos que permiten su operación.

Tabla 20 resumen de recursos y prioridades

N°	Servicio	Procesos Relacionados	Prioridad			Recursos
			1 Alta	2 Media	3 Baja	
1	Internet	Operaciones	Alta	-	-	Los recursos relacionados están identificados en la lista de recursos
2	Interconexión de sedes	Operaciones	-	Media	-	Los recursos relacionados están identificados en la lista de recursos
3	Servicios gestionados	Operaciones	-	-	Baja	Los recursos relacionados están identificados en la lista de recursos

4.3 Análisis de riesgos

4.3.1 Identificación de recursos

Los recursos principales han sido identificados y se ha establecido un nivel de criticidad.

Tabla 21 Inventario de recursos por nivel de criticidad.

Recurso del sistema / componente /activo	Plataforma / SO / Versión (según corresponda)	Descripción	Criticidad	Categoría de Activo	SERVICIO
Cisco WS-C6509-E / Agg	Cisco / IOS/ 15.1(2)SY6	Switch de Agregación vss 1 Metro Ethernet	Alta	Equipo Core M.E	INTERNET
Cisco WS-C6509-E / Agg	Cisco / IOS/ 15.1(2)SY6	Switch de Agregación vss 2 Metro Ethernet	Alta		
Cisco WS-C6509-E / INT	Cisco / IOS/ 15.1(2)SY6	Router de Internet vss 1 Metro Ethernet	Alta		
Cisco WS-C6509-E / INT	Cisco / IOS/ 15.1(2)SY6	Router de Internet vss 2 Metro Ethernet	Alta		
Cisco WS-C6506 /ABR	Cisco /IOS/ 15.1(2)SY3	Switch concentrador Metro Ethernet	Alta	Equipo Agregador M.E	INTERNET / L2L /S.G
Huawei NE20E-S2F / ABR	Huawei / VRP / V800R007C10SPC10	Router concentrador Metro Ethernet	Alta		
Switch S5720-32X-EI-24S-AC	Huawei / VRP / V200R010C00SPC600	Swtich Cabecera Metro Ethernet	Alta		
cisco WS-C6504-E / NAP	Cisco /IOS/ 15.1(2)SY3	Router NAP	Media	Equipo NAP	INTERNET
Switch S5720-28X-LI-24S-AC	Huawei / VRP / V200R010C00SPC600	Switch de acceso Metro Ethernet	Alta	Equipo Acceso M.E	INTERNET / L2L /S.G
Router HUAWEI NE40E-X3	Huawei / VRP / V800R009C10SPC200	Router Tollgate MPLS	Alta	Equipo Core MPLS	INTERNET
Router Huawei NE40E-X8	Huawei / VRP / V800R007C00SPC100	Router Provider MPLS	Alta		
Router Huawei NE20E-S8	Huawei / VRP / V800R009C10SPC200	Router Provider Edge MPLS	Alta	Equipo Agregador MPLS	INTERNET / L2L /S.G
Router Huawei NE20E-S2F	Huawei / VRP / V800R009C10SPC200	Router Provider Edge MPLS	Alta		
Switch S5720-28X-LI-24S-AC	Huawei / VRP / V200R010C00SPC600	Switch de acceso MPLS	Alta	Equipo Acceso MPLS	INTERNET / L2L /S.G
Arbor Arbor CP	ArborOS / V6	Equípos de Protección contra DDoS	Media	Equipos Anti DDoS	INTERNET

Arbor Arbor SW	ArborOS / V6	Equípos de Protección contra DDoS	Media		
Arbor Arbor TMS 2810	ArborOS / V6	Equipos de Protección contra DDoS	Media		
Arbor Arbor TMS2301	ArborOS / V6	Equipos de Protección contra DDoS	Media		
Servidor NTP-MPLS	Linux	Servidor de sincronización de hora	Baja	Servidores de soporte al backbone	INTERNET / L2L /S.G
Servidor Syslog MPLS	Linux	Gestión y análisis de logs de equipos Backbone	Baja		
Servidor Syslog Metro	Linux	Gestión y análisis de logs de equipos Backbone	Baja		
Servidor Tacacs	Linux	Servidor de autenticación	Media		
Interruptor de Transferencia de Fuente	Eaton STS 16	Interruptor de Transferencia de Fuente	Media	Interruptor de Transferencia de Fuente	INTERNET / L2L /S.G
Generador Eléctrico Honda	Honda	Generador Eléctrico	Media	Generador Eléctrico	INTERNET / L2L /S.G
Generador Eléctrico Honda	Honda 5 kw	Generador Eléctrico	Media		
UPS EMERSON GXT3-3000RT230	EMERSON GXT3-3000RT230	Sistema de alimentación ininterrumpida	Media	UPS	INTERNET / L2L /S.G
UPS EMERSON GXT3-3000RT230	EMERSON GXT3-6000RT230	Sistema de alimentación ininterrumpida	Media		
UPS EATON EX 2200 RT	EATON EX 2200 RT	Sistema de alimentación ininterrumpida	Media		
UPS EMERSON Liebert APM	EMERSON Liebert APM	Sistema de alimentación ininterrumpida	Media		
UPS EATON EX 3000 RT	EATON EX 3000 RT	Sistema de alimentación ininterrumpida	Media		
UPS EATON PW9130I3000XLI	EATON PW9130I3000XLI	Sistema de alimentación ininterrumpida	Media		
UPS EATON EX 3000 RT	EATON EX 3000 RT	Sistema de alimentación ininterrumpida	Media		
Estabilizador	IEDA LCRT-30	Estabilizador de voltaje	Media	Estabilizador	INTERNET / L2L /S.G
Estabilizador	IEDA LCRT- 80	Estabilizador de voltaje	Media		
Estabilizador	IEDA LCRT-30 s/tta	Estabilizador de voltaje	Media		
Enlaces de Fibra Óptica	-	Enlaces de Fibra Óptica	Media	Enlace Físico FO	INTERNET / L2L /S.G

ISP 1	-	ISP Internacional 1 (Telxius)	Alta	ISP	INTERNET / L2L /S.G
ISP 2	-	ISP Internacional 2 (CenturyLink)	Alta		
Proveedores de Transporte Nacional	-	Proveedores de Transporte Nacional (INTERNEXA)	Alta	Proveedor de transporte	INTERNET / L2L /S.G
Proveedores de Transporte Nacional	-	Proveedores de Transporte Nacional (RDNFO)	Alta		
Personal especializado (CORE)	-	Personal Especializado	Alta	Personal	INTERNET / L2L /S.G
Personal especializado (NOC)	-	Personal Especializado	Alta		
Proveedor de energía eléctrica	-	Proveedor de energía eléctrica	Alta	Proveedor de energía eléctrica	INTERNET / L2L /S.G

Tabla 22 Leyenda de nivel de criticidad de los recursos.

Criticidad	Descripción	Consecuencias
Alta	a) Sus funciones solo pueden ser ejecutadas por un activo idéntico.	Graves pérdidas económicas
	b) Su ausencia es motivo de interrupción de proceso crítico de la empresa.	Implica consecuencias legales.
	c) Costo de interrupción alto.	Ocasiona daño a la imagen de la empresa.
Media	a) Sus funciones pueden ser ejecutadas manualmente por un periodo corto.	Podría ocasionar un perjuicio económico no significativo.
	b) Su ausencia podría ocasionar demoras en la ejecución de un proceso crítico.	No hay consecuencias legales.
	c) Costo de interrupción medio	No se afecta la imagen de la empresa.
Baja	a) Sus funciones pueden ser ejecutadas manualmente por un periodo prolongado.	Sin perjuicio económico.
	b) Su ausencia no afecta a ningún proceso crítico de la empresa.	No hay consecuencias legales.
	c) Costo de interrupción bajo	No se afecta a la imagen de la empresa.

4.3.2 Evaluación de riesgos:

Tabla 23 Evaluación de riesgos por procesos de negocio.

Clase de Recurso	Amenaza	Servicio	Área	Probabilidad	Confidencialidad	Integridad	Disponibilidad	Impacto	Nivel de Riesgo	Nivel de Tolerancia	Código de Riesgo
Equipo Core M.E	Acceso no autorizado	INTERNET	CORE	Baja	2	2	2	Medio	Medio	Moderado	REDES-R001
Equipo Core M.E	Inundación / Daños por agua	INTERNET	CORE	Baja	1	3	3	Alto	Medio	Moderado	REDES-R002
Equipo Core M.E	Fuego / Incendio	INTERNET	CORE	Baja	1	3	3	Alto	Medio	Moderado	REDES-R003
Equipo Core M.E	Errores de configuración	INTERNET	CORE	Baja	0	2	3	Medio	Medio	Moderado	REDES-R004
Equipo Core M.E	Hardware sin soporte de fabricante	INTERNET	CORE	Media	0	0	1	Bajo	Medio	Moderado	REDES-R005
Equipo Core M.E	Ataque DDoS	INTERNET	CORE	Alta	0	0	3	Medio	Alto	Intolerable	REDES-R006
Equipo Core M.E	Terremoto	INTERNET	CORE	Baja	1	3	3	Alto	Medio	Moderado	REDES-R007
Equipo Core M.E	Incumplimiento de SLA	INTERNET	CORE	Media	0	0	3	Medio	Alto	Intolerable	REDES-R008
Equipo Agregador M.E	Acceso no autorizado	INTERNET / L2L /SG	CORE	Baja	2	2	2	Medio	Medio	Moderado	REDES-R009
Equipo Agregador M.E	Inundación / Daños por agua	INTERNET / L2L /SG	CORE	Baja	3	3	3	Alto	Medio	Moderado	REDES-R010
Equipo Agregador M.E	Errores de configuración	INTERNET / L2L /SG	CORE	Baja	0	2	2	Medio	Medio	Moderado	REDES-R011
Equipo Agregador M.E	Terremoto	INTERNET / L2L /SG	CORE	Baja	1	3	3	Alto	Medio	Moderado	REDES-R012
Equipo Agregador M.E	Fuego / Incendio	INTERNET / L2L /SG	CORE	Baja	1	3	3	Alto	Medio	Moderado	REDES-R013

Equipo Agregador M.E	Fluctuaciones o Corte del suministro eléctrico	INTERNET / L2L /SG	CORE	Baja	0	0	3	Medio	Medio	Moderado	REDES-R014
Equipo NAP	Indisponibilidad de Servicio	INTERNET	CORE	Baja	0	0	3	Medio	Medio	Moderado	REDES-R015
Equipo NAP	Incumplimiento de SLA	INTERNET	CORE	Baja	0	0	3	Medio	Medio	Moderado	REDES-R016
Equipo NAP	Ataque DDoS	INTERNET	CORE	Media	0	0	2	Bajo	Medio	Moderado	REDES-R017
Equipo NAP	Terremoto	INTERNET	CORE	Baja	0	0	3	Medio	Medio	Moderado	REDES-R018
Equipo Acceso M.E	Falla en Equipo de comunicación	INTERNET / L2L /SG	CORE	Baja	2	2	2	Medio	Medio	Moderado	REDES-R019
Equipo Core MPLS	Inundación / Daños por agua	INTERNET	CORE	Baja	1	3	3	Alto	Medio	Moderado	REDES-R020
Equipo Core MPLS	Fuego / Incendio	INTERNET	CORE	Baja	1	3	3	Alto	Medio	Moderado	REDES-R021
Equipo Core MPLS	Errores de configuración	INTERNET	CORE	Baja	0	2	3	Medio	Medio	Moderado	REDES-R022
Equipo Core MPLS	Hardware sin soporte de fabricante	INTERNET	CORE	Baja	2	2	2	Medio	Medio	Moderado	REDES-R023
Equipo Core MPLS	Ataque DDoS	INTERNET	CORE	Alta	0	0	3	Medio	Alto	Intolerable	REDES-R024
Equipo Core MPLS	Terremoto	INTERNET	CORE	Baja	1	3	3	Alto	Medio	Moderado	REDES-R025
Equipo Core MPLS	Incumplimiento de SLA	INTERNET	CORE	Media	0	0	3	Medio	Alto	Intolerable	REDES-R026
Equipo Agregador MPLS	Terremoto	INTERNET / L2L /SG	CORE	Baja	2	2	3	Alto	Medio	Moderado	REDES-R027

Equipo Agregador MPLS	Acceso no autorizado	INTERNET / L2L /SG	CORE	Muy Baja	0	0	2	Bajo	Bajo	Tolerable	REDES-R028
Equipo Agregador MPLS	Inundación / Daños por agua	INTERNET / L2L /SG	CORE	Baja	1	3	3	Alto	Medio	Moderado	REDES-R029
Equipo Agregador MPLS	Errores de configuración	INTERNET / L2L /SG	CORE	Baja	0	0	2	Bajo	Bajo	Tolerable	REDES-R030
Equipo Agregador MPLS	Terremoto	INTERNET / L2L /SG	CORE	Baja	0	0	2	Bajo	Bajo	Tolerable	REDES-R031
Equipo Agregador MPLS	Fuego / Incendio	INTERNET / L2L /SG	CORE	Baja	0	0	2	Bajo	Bajo	Tolerable	REDES-R032
Equipo Agregador MPLS	Fluctuaciones o Corte del suministro eléctrico	INTERNET / L2L /SG	CORE	Baja	0	0	2	Bajo	Bajo	Tolerable	REDES-R033
Equipo Acceso MPLS	Falla en Equipo de comunicación	INTERNET / L2L /SG	CORE	Baja	2	2	2	Medio	Medio	Moderado	REDES-R034
ISP	Indisponibilidad de Servicio	INTERNET	CORE	Baja	0	0	3	Medio	Medio	Moderado	REDES-R035
ISP	Incumplimiento de SLA	INTERNET	CORE	Baja	0	0	3	Medio	Medio	Moderado	REDES-R036
ISP	Ataque DDoS	INTERNET	NOC	Alta	0	0	3	Medio	Alto	Intolerable	REDES-R037
ISP	Terremoto	INTERNET	CORE	Baja	0	0	3	Medio	Medio	Moderado	REDES-R038
Proveedor de transporte	Indisponibilidad de Servicio	INTERNET / L2L /SG	CORE	Baja	0	0	3	Medio	Medio	Moderado	REDES-R039
Proveedor de transporte	Incumplimiento de SLA	INTERNET / L2L /SG	CORE	Baja	0	0	3	Medio	Medio	Moderado	REDES-R040
Proveedor de	Ataque DDoS	INTERNET / L2L /SG	CORE	Baja	0	0	2	Bajo	Bajo	Tolerable	REDES-R041

transporte											
Proveedor de transporte	Terremoto	INTERNET / L2L /SG	CORE	Baja	0	0	3	Medio	Medio	Moderado	REDES-R042
Personal Especializado	Indisponibilidad del personal por enfermedad o fallecimiento	INTERNET / L2L /SG	CORE	Media	0	0	3	Medio	Alto	Intolerable	REDES-R043
Equipos Anti DDoS	Falla en Equipo especializados de seguridad	INTERNET	CiberSOC	Muy Baja	0	0	3	Medio	Bajo	Tolerable	REDES-CS01
Equipos Anti DDoS	Errores de configuración	INTERNET	CiberSOC	Baja	0	3	3	Medio	Medio	Moderado	REDES-CS02
Equipos Anti DDoS	Terremoto	INTERNET	CiberSOC	Media	0	0	3	Medio	Alto	Intolerable	REDES-CS03
Equipos Anti DDoS	Fuego / Incendio	INTERNET	CiberSOC	Baja	0	0	3	Medio	Medio	Moderado	REDES-CS04
Servidores de soporte al backbone	Acceso no autorizado	INTERNET / L2L /SG	TI	Baja	1	2	2	Medio	Medio	Moderado	I.TI-T01
Servidores de soporte al backbone	Terremoto	INTERNET / L2L /SG	TI	Baja	0	1	2	Medio	Medio	Moderado	I.TI-T01
Servidores de soporte al backbone	Fuego / Incendio	INTERNET / L2L /SG	TI	Baja	0	3	1	Medio	Medio	Moderado	I.TI-T01

Servidores de soporte al backbone	Perdida de Suministro de Energia Electrica	INTERNET / L2L /SG	TI	Baja	0	3	3	Medio	Medio	Moderado	I.TI-T01
Interruptor de Transferencia de Fuente	Falla en Equipo de proteccion energia electrica	INTERNET / L2L /SG	Infraestructura de Red	Baja	0	0	3	Medio	Medio	Moderado	I.R-I01
Interruptor de Transferencia de Fuente	Terremoto	INTERNET / L2L /SG	Infraestructura de Red	Media	0	0	3	Medio	Alto	Intolerable	I.R-I02
Interruptor de Transferencia de Fuente	Fuego / Incendio	INTERNET / L2L /SG	Infraestructura de Red	Baja	0	0	3	Medio	Medio	Moderado	I.R-I03
Interruptor de Transferencia de Fuente	Fluctuaciones o Corte del suministro eléctrico	INTERNET / L2L /SG	Infraestructura de Red	Baja	0	0	2	Bajo	Bajo	Tolerable	I.R-I04
UPS	Fuego / Incendio	INTERNET / L2L /SG	Infraestructura de Red	Baja	0	0	2	Bajo	Bajo	Tolerable	I.R-I05
UPS	Fluctuaciones o Corte del suministro eléctrico	INTERNET / L2L /SG	Infraestructura de Red	Media	0	0	3	Medio	Alto	Intolerable	I.R-I06
UPS	Inundación / Daños por agua	INTERNET / L2L /SG	Infraestructura de Red	baja	0	0	2	Bajo	Bajo	Tolerable	I.R-I07
UPS	Terremoto	INTERNET / L2L /SG	Infraestructura de Red	Media	0	0	3	Medio	Alto	Intolerable	I.R-I08

Proveedor de enegia electrica	Perdida de Suministro de Energia Electrica	INTERNET / L2L /SG	Infraestructura de Red	Media	0	0	3	Medio	Alto	Intolerable	I.R-I09
Enlace Físico FO	Falla en Medio de comunicación	INTERNET / L2L /SG	Infraestructura de Red	Media	0	0	2	Bajo	Medio	Moderado	I.R-I10
Enlace Físico FO	Terremoto	INTERNET / L2L /SG	Infraestructura de Red	Media	0	0	3	Medio	Alto	Intolerable	I.R-I11
Enlace Físico FO	Daños por terceros	INTERNET / L2L /SG	Infraestructura de Red	Media	0	0	2	Bajo	Medio	Moderado	I.R-I12

4.3.3 Tratamiento de riesgos

Tabla 24 Tratamiento de los riegos.

Clase de Activo	Amenaza	Servicio	Gerencia	Área	Probabilidad	Confidencialid	Integridad	Disponibilidad	Impacto	Nivel de Riesgo	Nivel de Tolerancia	Código de Riesgo	Tareas para realizar	Periodo de ejecución	Dueño del Riesgo
Equipo Core M.E	Ataque DDoS	Internet	REDES	Core	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	REDES-R006	1) Supervisar el cumplimiento de los contratos con el proveedor. 2) Asegurar el cumplimiento del procedimiento para la mitigación.	Ago-19	Gerente de redes
Equipo Core M.E	Incumplimiento de SLA	Internet	REDES	Core	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	REDES-R008	1) Supervisar el cumplimiento de los contratos con los proveedores. 2) Asegurar el cumplimiento de procedimientos de configuración de equipos Core. 3) Contar con equipos de spare en el almacén.	Set-19	Gerente de redes
Equipo Core MPLS	Ataque DDoS	Internet	REDES	Core	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	REDES-R024	1) Supervisar el cumplimiento de los contratos con el proveedor. 2) Asegurar el cumplimiento del procedimiento para la mitigación.	Ago-19	Gerente de redes
Equipo Core MPLS	Incumplimiento de SLA	Internet	REDES	Core	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	REDES-R026	1) Supervisar el cumplimiento de los contratos con los proveedores. 2) Asegurar el cumplimiento de procedimientos de configuración de equipos core. 3) Contar con equipos de spare en el almacén.	Set-19	Gerente de redes
ISP	Ataque DDoS	Internet	REDES	NOC	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	REDES-R037	1) Supervisar el cumplimiento de los contratos con el proveedor. 2) Asegurar el cumplimiento del procedimiento para la mitigación.	Ago-19	Gerente de redes
Personal Especializado	Indisponibilidad del personal por enfermedad o fallecimiento	INTERNET / L2L /SG	REDES	TODOS	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	REDES-R043	2) Gestionar Contratos de Servicio de Soporte de Personal especializado con Proveedores Especializados.	Ago-19	Gerente de redes

Equipos Anti DDoS	Terremoto	INTERNET	REDES	Ciber SOC	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	REDES-CS03	1) Realizar mitigaciones mediante el servicio de Blackhole remoto, mientras se repone el equipo averiado.	Ago-19	Gerente de redes
Interruptor de Transferencia de Fuente	Terremoto	INTERNET / L2L /SG	Infraestructura de Red	Infraestructura de Red	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	I.R-I02	1) Probar escenario de alta disponibilidad en datacenter de respaldo.	Ago-19	Gerencia de Datacenter y nodos
UPS	Fluctuaciones o Corte del suministro eléctrico	INTERNET / L2L /SG	Infraestructura de Red	Infraestructura de Red	**Alta**	0	0	3	**Medio**	**Alto**	**Intolerable**	I.R-I06	1) Probar escenario de alta disponibilidad en datacenter de respaldo.	Ago-19	Gerencia de Datacenter y nodos
UPS	Terremoto	INTERNET / L2L /SG	Infraestructura de Red	Infraestructura de Red	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	I.R-I08	1) Probar escenario de alta disponibilidad en datacenter de respaldo.	Ago-19	Gerencia de Datacenter y nodos
Proveedor de energía eléctrica	Perdida de Suministro de energía eléctrica	INTERNET / L2L /SG	Infraestructura de Red	Infraestructura de Red	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	I.R-I09	1) Implementación de un sistema de alimentación continua. . 2) Contratar un proveedor de grupos electrógenos para cortes de energía prolongados.	Ago-19	Gerencia de Datacenter y nodos
Enlace Físico FO	Terremoto	INTERNET / L2L /SG	Infraestructura de Red	Infraestructura de Red	**Media**	0	0	3	**Medio**	**Alto**	**Intolerable**	I.R-I11	1) Probar escenario de alta disponibilidad mediante enlaces de respaldo	Ago-19	Gerencia de Datacenter y nodos

4.3.4 Riesgos residuales

Tabla 25 Análisis de riesgos residuales.

Clase de Activo	Amenaza	Servicio	Probabilidad	Impacto	Nivel de Riesgo	Nivel de Tolerancia	Estrategia	Acciones	Periodo de revisión	Responsables
Equipo Core M.E	Ataque DDoS	Internet	**Media**	**Medio**	**Alto**	**Intolerable**	Transferir	Se contrata servicio de mitigación en la nube con Arbor Cloud.	Anual	CiberSoc
Equipo Core M.E	Incumplimiento de SLA	Internet	**Media**	**Medio**	**Alto**	**Intolerable**	Mitigar (reducir)	Contar con equipos de Spare en el almacén.	Trimestral	NOC
Equipo Core MPLS	Ataque DDoS	Internet	**Media**	**Medio**	**Alto**	**Intolerable**	Transferir	Se contrata servicio de mitigación en la nube con Arbor Cloud.	Anual	CiberSoc
Equipo Core MPLS	Incumplimiento de SLA	Internet	**Media**	**Medio**	**Alto**	**Intolerable**	Transferir	Contar con equipos de Spare en el almacén.	Trimestral	NOC
ISP	Ataque DDoS	Internet	**Media**	**Medio**	**Alto**	**Intolerable**	Mitigar (reducir)	- Se contrata servicio de mitigación en la nube con Arbor Cloud. - Se implementa servicio de blackhole	Trimestral	NOC
Personal Especializado	Indisponibilidad del personal por enfermedad o fallecimiento	INTERNET / L2L /SG	**Media**	**Medio**	**Alto**	**Intolerable**	Transferir	Se realiza contrato con empresa especializada para cubrir puestos de personal ausente	Anual	Gerencias
Equipos Anti DDoS	Terremoto	INTERNET	**Media**	**Medio**	**Alto**	**Intolerable**	Mitigar (reducir)	Se utiliza servicio de blackhole remoto	Trimestral	NOC
Interruptor de Transferencia de Fuente	Terremoto	INTERNET / L2L /SG	**Media**	**Medio**	**Alto**	**Intolerable**	Mitigar (reducir)	Se activa el datacenter alterno.	Anual	Infraestructura de red
UPS	Fluctuaciones o Corte del suministro eléctrico	INTERNET / L2L /SG	**Media**	**Medio**	**Alto**	**Intolerable**	Mitigar (reducir)	Se activa el datacenter alterno.	Anual	Infraestructura de red
UPS	Terremoto	INTERNET / L2L /SG	**Media**	**Medio**	**Alto**	**Intolerable**	Mitigar (reducir)	Se activa el sitio alterno.	Anual	Infraestructura de red
Proveedor de energía eléctrica	Perdida de Suministro de Energía Eléctrica	INTERNET / L2L /SG	**Media**	**Medio**	**Alto**	**Intolerable**	Mitigar (reducir)	Activar sistemas de generador eléctrico. - Se activar el datacenter alterno.	Anual	Infraestructura de red
Enlace Físico FO	Falla en Medio de comunicación	INTERNET / L2L /SG	**Media**	**Medio**	**Alto**	**Intolerable**	Mitigar (reducir)	Activar enlaces de respaldo (rutas diferenciadas)	Anual	Emergencias de F.O

4.4 Controles preventivos

En esta sección se identifican algunos controles preventivos, que pueden ser aplicados a fin de evitar desastres:

- Contar con un sistema de fuentes de alimentación interrumpida (UPS) en cada nodo y datacenter, con una capacidad adecuada para proporcionar energía eléctrica a todos los componentes en periodos cortos.
- Contar con generadores eléctricos estacionarios y portátiles para proporcionar energía eléctrica por periodos prolongados.
- Contar con un sistema de aire acondicionado en cada nodo y datacenter, a fin de evitar fallas de componentes de equipos críticos a causa de un incremento de temperatura.
- Contar con sistemas de extinción de incendios adecuados para ambientes donde se alojan equipos electrónicos.
- Contar con sensores de humo y se humedad en cada nodo y datacenter.
- Almacenamiento externo de medios de respaldo, registros no electrónicos y documentación del sistema.
- Contar con sistemas de control de acceso para herramientas, sistemas y documentaciones.
- Contar con equipos redundantes a nivel de fuentes de poder, tarjetas y controladoras.

4.5 Escenarios de desastre

Se determinaron los siguientes escenarios ante incidentes disruptivos:

Escenario 1: Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias.
Escenario 2: Ataque DDoS mayor a 20Gbps y/o por más de 10 horas.
Escenario 3: Incendio que afecta local del Data Center principal (DC1).
Escenario 4: Inundación que afecta el Local del Data Center Principal (DC1).
Escenario 5: Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1).
Escenario 6: Ausencia de personal especializado por fallecimiento o enfermedad.

Tabla 26 Escenario de desastre 1.

ESCENARIO 1	PROCESOS DE NEGOCIO AFECTADOS	IMPACTOS POTENCIALES	TIEMPO DE INACTIVIDAD MÁXIMO TOLERABLE (MTD)	COMPONENTES AFECTADOS	TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)
Sismo mayor a 6 hasta 8 grados	Servicio de Acceso dedicado a Internet	a) Perder la comunicación con los proveedores internacionales (físico). b) Indisponibilidad de los servicios en el Data Center (físico) c) Indisponibilidad de los servicios de acceso en todos los nodos. (físico) d) Indisponibilidad entre interconexión entre Data Center. (físico) e) Indisponibilidad de Servicios de DNS. (físico)	4 horas	a) Local Principal. b) Data Center Principal.	2 horas
	Servicio de Interconexión de Sedes	a) Indisponibilidad de los servicios en el Data Center b) Indisponibilidad de los servicios de acceso en todos los nodos. c) Indisponibilidad entre interconexión entre Data Center.	6 horas	a) Local Principal. b) Data Center Principal	6 horas
	Servicios Gestionados	a) Perder la comunicación con los proveedores internacionales. b) Indisponibilidad de los servicios de acceso en todos los nodos. c) Indisponibilidad entre interconexión entre Data Center. d) Indisponibilidad de Servicios de DNS.	6 horas	a) Local Principal. b) Data Center Principal	3 horas

Tabla 27 Escenario de desastre 2.

ESCENARIO 2	PROCESOS DE NEGOCIO AFECTADOS	IMPACTOS POTENCIALES	TIEMPO DE INACTIVIDAD MÁXIMO TOLERABLE (MTD)	COMPONENTES AFECTADOS	TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)
Ataque DDoS mayor a 20GB y/o por más de 10 horas	Servicio de Acceso dedicado a Internet	Indisponibilidad del servicio de internet.	4 horas	Servicio de Internet	2 horas
	Servicio de Interconexión de Sedes	Saturación de Canal	6 horas	Servicio de Internet	3 horas

	Servicios Gestionados	Indisponibilidad del servicio de internet. Saturación de Canal.	6 horas	Servicio de Internet	3 horas

Tabla 28 Escenario de desastre 3.

ESCENARIO 3	PROCESOS DE NEGOCIO AFECTADOS	IMPACTOS POTENCIALES	TIEMPO DE INACTIVIDAD MÁXIMO TOLERABLE (MTD)	COMPONENTES AFECTADOS	TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)
Incendio en local Principal que afecta al Data Center	Servicio de Acceso dedicado a Internet	Perdida de redundancia	4 horas	Local Principal Data Center Principal	2 horas
	Servicio de Interconexión de Sedes	Perdida de redundancia	6 horas	Local Principal Data Center Principal	3 horas
	Servicios Gestionados	Perdida de redundancia	6 horas	Local Principal Data Center Principal	3 horas

Tabla 29 Escenario de desastre 4

ESCENARIO 4	PROCESOS DE NEGOCIO AFECTADOS	IMPACTOS POTENCIALES	TIEMPO DE INACTIVIDAD MÁXIMO TOLERABLE (MTD)	COMPONENTES AFECTADOS	TIEMPO OBJETIVO DE RECUPERACIÓN (RTO
Inundación en Local Principal que afecta al Data Center.	Servicio de Acceso dedicado a Internet	Perdida de redundancia	4 horas	Local Principal Data Center Principal	2 horas
	Servicio de Interconexión de Sedes	Perdida de redundancia	6 horas	Local Principal Data Center Principal	3 horas
	Servicios Gestionados	Perdida de redundancia	6 horas	Local Principal Data Center Principal	3 horas

Tabla 30 Escenario de desastre 5

ESCENARIO 5	PROCESOS DE NEGOCIO AFECTADOS	IMPACTOS POTENCIALES	TIEMPO DE INACTIVIDAD MÁXIMO TOLERABLE (MTD)	COMPONENTES AFECTADOS	TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)
Pérdida de Suministro de Energía Eléctrica	Servicio de Acceso dedicado a Internet	Perdida de redundancia	4 horas	Local Principal Data Center Principal	2 horas

mayor a 6 horas que afecta el Data Center Principal.	Servicio de Interconexión de Sedes	Perdida de redundancia	6 horas	Local Principal Data Center Principal	3 horas
	Servicios Gestionados	Perdida de redundancia	6 horas	Local Principal Data Center Principal	3 horas

Tabla 31 Escenario de desastre 5

ESCENARIO 6	PROCESOS DE NEGOCIO AFECTADOS	IMPACTOS POTENCIALES	TIEMPO DE INACTIVIDAD MÁXIMO TOLERABLE (MTD)	COMPONENTES AFECTADOS	TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)
Ausencia de personal especializado por fallecimiento o enfermedad.	Servicio de Acceso dedicado a Internet	Aumento en el tiempo de resolución de un incidente de tipo mayor.	4 horas	Atención del Servicio	2 horas
	Servicio de Interconexión de Sedes	Aumento en el tiempo de resolución de un incidente de tipo mayor.	6 horas	Atención del Servicio	3 horas
	Servicios Gestionados	Aumento en el tiempo de resolución de un incidente de tipo mayor.	6 horas	Atención del Servicio	3 horas

4.6 Estrategias de contingencias

Escenario	Sismo mayor a 6 hasta 8 grados que afecta el local principal y los secundarios.
Servicios	Internet, interconexión de sedes y Servicios Gestionados.
Código	E001
Estrategia	
La ejecución de esta estrategia dependerá de la siguiente premisa: ***"El sismo no afecto la infraestructura de fibra óptica"*** **Durante Jornada Laboral** En caso el Sismo ocurra durante el horario laboral se seguirán las recomendaciones descritas en el ***Plan de emergencia*** para salvaguardar la vida de las personas. Asimismo, se considera las recomendaciones dadas por el Instituto Nacional de Defensa Civil en los medios de comunicación (radio, televisión), las herramientas WEB 2.0 (Twitter Oficial) o mensajes de texto que pudieran enviar. En caso el desastre haya afectado completamente las instalaciones de trabajo de manera permanente se utilizará el servicio de oficina de Gálvez 2 y/o Gálvez 1 por plazo indeterminado.	

El equipo de respuesta ante incidentes realizará la habilitación de las conexiones físicas y lógicas para comunicación de la red backbone.

El equipo de respuesta ante incidentes realizara las interconexiones con los proveedores internacionales.

El equipo de respuesta ante incidentes verificará el funcionamiento de los servicios.

El equipo de respuesta ante incidentes informara al TAC que el servicio esta reestablecido.

El equipo de respuesta ante incidentes informará al Comité de Crisis que el servicio esta reestablecido.

Para el reporte de incidentes de la Mesa de Ayuda se comunicará telefónicamente y se anotará en el formato de registro definido mientras reestablece los sistemas de gestión (Service Desk).

Las partes interesadas serán comunicadas por los canales de comunicación establecidos y por el Líder o Suplentes del Equipo de Comunicaciones.

Después de la Jornada Laboral

En caso el sismo ocurra después de la jornada laboral, los colaboradores acudirán a laborar en el local de la oficina de Gálvez 2 y/o Gálvez 1 lo que será informado por medio de los canales de comunicación establecidos.

Vuelta a la normalidad
Se comunicará por los medios establecidos a todo el personal la vuelta a la normalidad una vez que el local afectado quede operativo para el normal funcionamiento de sus operaciones.

Escenario	Ataque DDoS mayor a 20Gbps y/o por más de 10 horas.
Servicios	Internet
Código	E002
Estrategia: Mitigación de tipo DDoS con Arbor Cloud	
Se dispone de un monitoreo de 24x7 de la infraestructura por parte del are NOC. El equipo de respuesta ante incidentes identificará al destino que está siendo atacado con un ataque de Denegación de Servicios Distribuido DDoS. El equipo de respuesta ante incidentes realizara la acción de redirigir el tráfico de internet hacia la Nube de nuestro Proveedor de Protección contra ataques DDoS. El equipo de respuesta ante incidentes supervisará que se mantenga la comunicación con el proveedor para ver el seguimiento del ticket de atención. El equipo de respuesta ante incidentes consolidará en una bitácora toda la información con respecto al incidente y elabora un informe para el cliente sobre la afectación del servicio.	

El servicio de mitigación en la nube cuenta con la capacidad de mitigar el tráfico malicioso hasta 11 Tbps por un periodo de 72 horas y se cuenta hasta 6 mitigaciones por año, en caso se haya consumido las 6 mitigaciones se deberá optar por la estrategia 2.1.
Vuelta a la normalidad
El equipo de respuesta ante incidentes realizará pruebas para validar el correcto funcionamiento de los servicios. El equipo de respuesta ante incidentes solicitará detener la mitigación en la nube. El equipo de respuesta ante incidentes comunicará al TAC que la mitigación ha finalizado.

Escenario	Ataque DDoS mayor a 20Gbps y/o por más de 10 horas.
Servicios	Internet
Código	E002.1
Estrategia: Mitigación de tipo DDoS con Black Hole Remoto	
Esta estrategia deberá ser usada cuando las 6 mitigaciones en la nube hayan sido usadas. Se dispone de un monitoreo de 24x7 de la infraestructura por parte del are NOC. El equipo de respuesta ante incidentes identificará al destino que está siendo atacado con un ataque de Denegación de Servicios Distribuido DDoS. El equipo de respuesta ante incidentes realizara la acción de enrutar la dirección IP atacada mediante BGP hacia el servicio de blackhole remoto con el proveedor Telxius. El equipo de respuesta ante incidentes abrirá un ticket con el proveedor a fin de monitorear el tráfico cada 60 minutos. El equipo de respuesta ante incidentes consolidará en una bitácora toda la información con respecto al incidente y elabora un informe para el cliente sobre la afectación del servicio.	
Vuelta a la normalidad	
El equipo de respuesta ante incidentes dejará de anunciar el prefijo /32 hacia el blackhole remoto. bEl equipo de respuesta ante incidentes realizará pruebas para validar el correcto funcionamiento de los servicios. El equipo de respuesta ante incidentes comunicará al TAC que la mitigación ha finalizado.	

Escenario	Incendio que afecta local del Data Center principal (DC1).
Servicios	Internet, interconexión de sedes y Servicios Gestionados.
Código	E003
Estrategia	
Durante la jornada laboral En caso el incendio ocurra durante el horario laboral se seguirán las recomendaciones descritas en el ***Plan de emergencia*** para salvaguardar la vida de las personas.	

En caso el desastre haya afectado completamente las instalaciones de trabajo de manera permanente se utilizará la oficina Gálvez 2 por plazo indeterminado.

El equipo de respuesta ante incidentes validará que todos los servicios se encuentren operando desde el Datacenter 2 (Galvez 1).

El equipo de respuesta evaluará los daños causados por el incidente.

Para el reporte de incidentes se comunicará telefónicamente y se anotará en el formato de registro definido mientras restablece la copia de seguridad de la herramienta de gestión de incidentes.

Las partes interesadas serán comunicadas por los canales de comunicación establecidos y por el Líder o Suplentes del Equipo de Comunicaciones.

Después de la Jornada Laboral

En caso el incendio ocurra después de la jornada laboral, los colaboradores acudirán a laborar en el local Gálvez 2 lo que será informado por medio de los canales de comunicación establecidos.

Vuelta a la normalidad
Se comunicará por los medios establecidos a los colaboradores la vuelta a la normalidad una vez que el local quede operativo para el normal funcionamiento de sus operaciones. El equipo de respuesta realizará las acciones y pruebas necesarias para activar todos los servicios nuevamente en el Data Center 1 según los procedimientos establecidos.

Escenario	Inundación que afecta el Local del Data Center Principal (DC1).
Servicios	Internet, interconexión de sedes y Servicios Gestionados.
Código	E004
Estrategia	

Durante la jornada laboral

En caso el incendio ocurra durante el horario laboral se seguirán las recomendaciones descritas en el ***Plan de emergencia*** para salvaguardar la vida de las personas.

En caso el desastre haya afectado completamente las instalaciones de trabajo de manera permanente se utilizará la oficina Gálvez 2 por plazo indeterminado.

El equipo de respuesta ante incidentes validará que todos los servicios se encuentren operando desde el Datacenter 2 (Galvez 1).

El equipo de respuesta evaluará los daños causados por el incidente.

El equipo de Respuesta ante incidentes realizará las coordinaciones para que se contrate el servicio de motobomba para que retire el agua causada por el aniego en todo el local principal.

El equipo de Respuesta ante incidentes evaluará luego que se realice la succión del agua causada por el aniego en todo el local principal que las instalaciones queden operativas y sobre todo que no existan riesgos para la salud y vida de las personas.

Después de la Jornada Laboral

En caso el incendio ocurra después de la jornada laboral, los colaboradores acudirán a laborar en el local Gálvez 2 lo que será informado por medio de los canales de comunicación establecidos.

Vuelta a la normalidad

Se comunicará por los medios establecidos a los colaboradores la vuelta a la normalidad una vez que el local quede operativo para el normal funcionamiento de sus operaciones.
El equipo de respuesta realizará las acciones y pruebas necesarias para activar todos los servicios nuevamente en el Data Center 1 según los procedimientos establecidos.

Escenario	Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1).
Servicios	Internet, interconexión de sedes y Servicios Gestionados.
Código	E005

Estrategia

Durante la jornada laboral

El personal de Construcción y Mantenimiento de Infraestructura de Red verificará si el corte de suministro de energía afecta a toda a la zona mediante comunicación telefónica con la empresa proveedora de suministro de energía con la finalidad de estimar el tiempo en que el servicio volvería a estar disponible y lo comunicará al Gerente de Construcción y Mantenimiento de Infraestructura de Red.

Si la interrupción es mayor a 6 horas, el Comité de Crisis por medio de los canales establecidos comunicará a los colaboradores que deberá laborar desde su casa o trasladarse al local de Gálvez 2, bajo la responsabilidad del Gerente de Operaciones.

El equipo de Respuesta ante incidentes activará el generador de la sede principal según el procedimiento establecido.

El equipo de Respuesta ante incidentes trasladará el generador móvil hacia la sede principal.

El equipo de Respuesta ante incidentes, transcurridas las 6 horas encenderá el generador móvil para alternar con el generador de la sede principal.

El equipo de Respuesta ante incidentes coordinará con un proveedor externo para contar con un tercer generador de tipo móvil.

Después de la Jornada Laboral
En caso la falta de suministro ocurra después de la jornada laboral y dure hasta el día siguiente, los colaboradores acudirán a laborar en el local Gálvez 2 o trabajaran desde su casa lo que será informado por medio de los canales de comunicación establecidos.

Vuelta a la normalidad

Se comunicará por los medios establecidos a todo el personal que el suministro de energía eléctrica se ha restablecido para que pueda retornar a la oficina.

Escenario	Ausencia de personal especializado por fallecimiento o enfermedad.
Servicios	Internet, interconexión de sedes y Servicios Gestionados.
Código	E006

Estrategia

Personal especializado de Networking

Para el caso del personal especializado de Netoworking, se dispone de acuerdos formales con empresas especializadas en las marcas de los equipos de comunicaciones desplegados.

Estos proveedores según marca de equipos están identificados en la lista de proveedores.

Según se determine la causa del a ausencia de personal especializado el Equipo de Respuesta ante incidentes coordinara con el proveedor especializado para la provisión del personal necesario según la marca del equipo de comunicaciones por el tiempo que sea necesario.

El personal especializado asignado será informado por el Equipo de Respuesta ante Incidentes de la situación de los requerimientos, peticiones o incidentes según sea los casos relacionados a los servicios de Internet, Interconexión de Sedes y Servicios Gestionados.

En caso de que la causa de ausencia de personal especializado sea por fallecimiento o enfermedad permanente, el jefe del área informará a Recursos Humanos para brindar soporte a los familiares directos del colaborador afectado, además de iniciar un proceso de selección de personal según los procedimientos establecidos en la organización.

Personal especializado de seguridad informática

Para el caso del personal especializado de seguridad informática dispone de acuerdos formales con empresas especializadas en las marcas de los equipos seguridad desplegados.

Estos proveedores según marca de equipos están identificados en la lista de proveedores.

Según se determine la causa del a ausencia de personal especializado el Equipo de Respuesta ante incidentes coordinara con el proveedor especializado para la provisión del personal necesario según la marca del equipo de seguridad informática por el tiempo que sea necesario.

El personal especializado asignado será informado por el Equipo de Respuesta ante Incidentes de la situación de los requerimientos, peticiones o incidentes según sea los casos relacionados a los servicios de Internet, Interconexión de Sedes y Servicios Gestionados.

En caso de que la causa de ausencia de personal especializado sea por fallecimiento o enfermedad permanente, el jefe del área informará a Recursos Humanos para brindar soporte a los familiares directos del colaborador afectado, además de iniciar un proceso de selección de personal según los procedimientos establecidos en la organización**.**

Vuelta a la normalidad

Una vez que el personal especializado se pueda reincorporar a sus labores el Equipo de Respuesta ante Incidentes informará el estado de los requerimientos, peticiones o incidentes

según sea los casos relacionados a los servicios de Internet, Interconexión de Sedes y Servicios Gestionados.

De ser el caso de nuevo personal que cubre plazas de personal especializado será capacitado en las herramientas y procedimientos que usa la organización para la gestión de requerimientos, peticiones o incidentes de los servicios de Internet, Interconexión de Sedes y Servicios Gestionados**.**

4.7 Proceso de ejecución de DRP

Para el proceso de ejecución del plan de recuperación ante desastres se seguirán las siguientes acciones:

1) Identificación de la emergencia: el área NOC es el área que realiza un monitoreo 24x7 y a donde se reportan todos los incidentes relacionados a los procesos de negocio, equipamiento y averías, por lo que esta área determinará si es necesario comunicar el suceso al comité de crisis o ejecutará las atenciones con el proceso normal de atención de avería.
2) Evaluación del comité de crisis: el comité de crisis tendrá una reunión de emergencia en la que se tomará la decisión a cerca de la declaratoria de emergencia.
3) Declaración de emergencia: una vez que el comité de crisis haya hecho la declaración de emergencia deberá activarse todos los protocolos establecidos para cada una de las situaciones.
4) Comunicación a los líderes de equipos de respuesta: Inmediatamente después de la declaratoria de emergencia se deberá comunicar con todos los equipos de respuesta mediante el árbol de comunicaciones, a fin de que cada integrante asuma su rol.
5) Ejecución de estrategias de DRP: cada integrante de cada equipo debe de conocer y ejecutar los lineamientos establecidos en las estrategias, así mismo debe mantener comunicación al líder de cada equipo, para que estos a su vez informen al comité de crisis.
6) Trabajos de retorno a la normalidad: Una vez que la emergencia haya sido superada, se debe ejecutar los trabajos para regresar al estado inicial con todos los procesos de negocio funcionando a su máxima capacidad y funcionalidad.
7) Fin de la declaratoria de emergencia: una vez que todo haya regresado a la normalidad, el comité de crisis dará por finalizado la declaratoria de emergencia, y se procederá a con la recopilación de información, lecciones aprendidas y el proceso de mantenimiento del DRP.

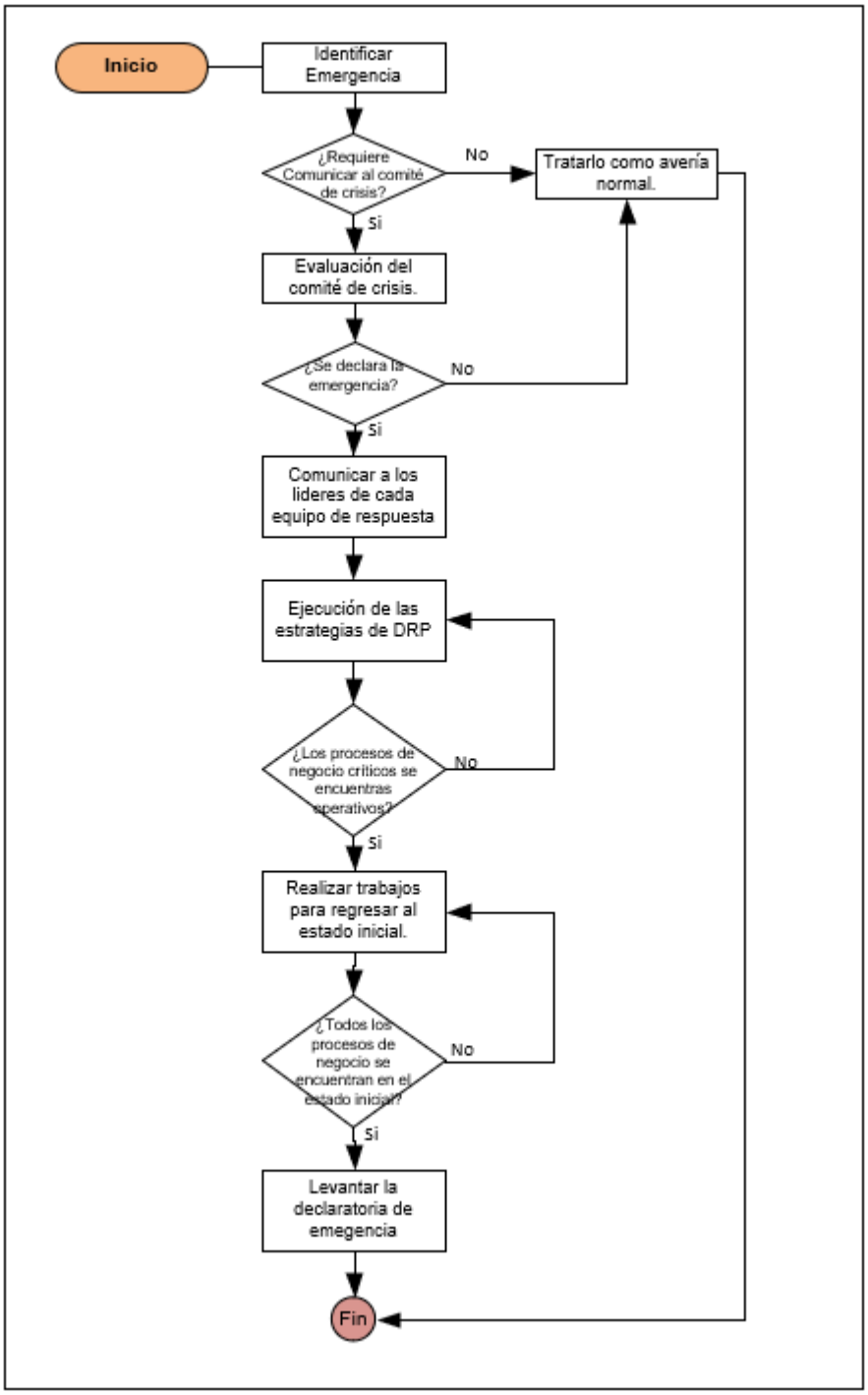


Figura 13 Flujo de ejecución de DRP

Fuente: Elaboración propia.

4.8 Recursos

Tabla 32 Recursos necesarios para el escenario 1

Recursos	Escenario 1: Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias.
Personas	-Todos los colaboradores
Informaciones y datos	-Información sobre el incidente -Datos de partes interesadas
Edificios, entorno de trabajo y servicios asociados	-Sede Galvez I -Sede Galvez II -Sede Krumdieck
Instalaciones, equipos y consumibles	-Combustible -Equipo de Fusión y Medición de Fibra Óptica -Unidad Móvil de Emergencia -Grupo Electrógeno Móvil
Sistemas de tecnología de la información y la comunicación	-Equipos de Comunicación -Equipos de Seguridad -Servidor de Monitoreo -Herramientas de Monitoreo -Herramienta de ITSM -Correo Electrónico -Software de Ofimática -Herramientas de Networking -Navegador Chrome -Sistema Operativo Windows
Transportes	-Publico (Taxi) -Privado -Camioneta de Emergencias.

Tabla 33 Recursos necesarios para el escenario 2

Recursos	Escenario 2: Ataque DDoS mayor a 20Gbps y/o por más de 10 horas.
Personas	-Jefe NOC -Analista de NOC -Supervisor NOC -Especialista Core -Especialista Senior de Seguridad
Informaciones y datos	-Manual de mitigación anti DDoS -Lista de contactos y escalamiento -Bitácora del incidente -Informe de Incidente
Edificios, entorno de trabajo y servicios asociados	-Sede Gálvez II

Instalaciones, equipos y consumibles	-Oficina de monitoreo NOC -Estaciones de Trabajo. -Monitores -Smartphone -Equipo especializado de seguridad Anti DDoS. -Equipo de Monitoreo
Sistemas de tecnología de la información y la comunicación	-Herramientas de Monitoreo -Herramienta de ITSM. -Correo Electrónico. -File Server. -Software de Ofimática -Herramientas de Networking -Navegador Chrome -Sistema Operativo Windows
Transportes	-Publico (Taxi) -Privado

Tabla 34 Recursos necesarios para el escenario 3

Recursos	Escenario 3: Incendio que afecta local del Data Center principal (DC1).
Personas	-Gerente de Datacenter y Nodos. -Jefe de Infraestructura de Datacenter y Nodos. -Analista de Infraestructura de Datacenter y Nodos. -Gerente de TI -Jefe de Infraestructura TI -Analista TI -Analista NOC -Analista TAC
Informaciones y datos	-Información sobre el incidente -Datos de partes interesadas
Edificios, entorno de trabajo y servicios asociados	-Sede Krumdieck
Instalaciones, equipos y consumibles	-Data Center 2 -Sistemas contra incendios -Extintores -Detectores de humo
Sistemas de tecnología de la información y la comunicación	-Herramientas de Monitoreo -Herramienta de ITSM. -Correo Electrónico. -File Server. -Software de Ofimática -Herramientas de Networking -Navegador Chrome -Sistema Operativo Windows

Transportes	-Publico (Taxi) -Privado -Camioneta de Emergencias

Tabla 35 Recursos necesarios para el escenario 4

Recursos	Escenario 4: Inundación que afecta el Local del Data Center Principal (DC1).
Personas	-Gerente de Datacenter y Nodos. -Jefe de Infraestructura de Datacenter y Nodos. -Analista de Infraestructura de Datacenter y Nodos. -Gerente de TI -Jefe de Infraestructura TI -Analista TI -Analista NOC -Analista TAC
Informaciones y datos	-Información sobre el incidente -Datos de partes interesadas
Edificios, entorno de trabajo y servicios asociados	-Sede Krumdieck
Instalaciones, equipos y consumibles	-Data Center 2 -Detectores de humedad -Sistema de bombeo de agua
Sistemas de tecnología de la información y la comunicación	-Herramientas de Monitoreo -Herramienta de ITSM. -Correo Electrónico. -File Server. -Software de Ofimática -Herramientas de Networking -Navegador Chrome -Sistema Operativo Windows
Transportes	-Publico (Taxi) -Privado -Camioneta de Emergencias

Tabla 36 Recursos necesarios para el escenario 5

Recursos	Escenario 5: Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1).
Personas	-Jefe de Infraestructura -Supervisor de Energía -Supervisor de Infraestructura -Gerente de TI -Supervisor NOC

Informaciones y datos	-Información sobre el incidente -Datos de partes interesadas
Edificios, entorno de trabajo y servicios asociados	-Sede Galvez I -Sede Galvez II
Instalaciones, equipos y consumibles	-Grupo Electrógeno -Grupo Electrógeno Movil -Herramientas de medición eléctrica
Sistemas de tecnología de la información y la comunicación	-Laptop -Smartphone
Transportes	-Publico (Taxi) -Privado -Camioneta de Emergencias

Tabla 37 Recursos necesarios para el escenario 6

Recursos	**Escenario 6: Ausencia de personal especializado por fallecimiento o enfermedad.**
Personas	-Analista de NOC. -Supervisor NOC. -Especialista Core. -Especialista Senior de Seguridad. -Técnico de Infraestructura -Supervisor de Energía -Supervisor de Infraestructura -Especialista de TI -Analista TAC
Informaciones y datos	-Información sobre el incidente -Datos de partes interesadas -Manuales y procedimientos -Lista de contactos y escalamientos.
Edificios, entorno de trabajo y servicios asociados	-Sede Galvez I -Sede Galvez II -Sede Krumdieck
Instalaciones, equipos y consumibles	-Centro de Operaciones NOC. -Estaciones de Trabajo. -Monitores. -Smartphone.

Sistemas de tecnología de la información y la comunicación	-Herramientas de Monitoreo -Herramienta de ITSM. -Correo Electrónico -File Server. -Software de Ofimática -Herramientas de Networking -Navegador Chrome -Sistema Operativo Windows
Transportes	-Publico (Taxi) -Privado

4.9 Roles y responsabilidades

En este capítulo se definen los roles y las responsabilidades que tendrá cada equipo antes durante y después de un evento disruptivo que implique la activación del DRP, los equipos están designados de manera tal que exista un respaldo de cada uno de los roles en caso se presente alguna dificultad con el personal designado.

1) Comité de Crisis:

   El Comité de Crisis tiene como objetivo principal asegurar la integridad física del personal durante un incidente que conduzca a una crisis, de la declaración de la crisis y activación de los planes de recuperación de ante desastres.

Tabla 38 Comité de crisis

ROL	INTEGRANTE	SUPLENTE 1	SUPLENTE 2
Líder del Equipo	Gerente General	Director Comercial	Gerente Post Venta
Integrantes del Equipo	Director de Operaciones	Gerente de redes	Gerente de Operación del Servicio
	Gerente TI	Jefe de Mesa de Ayuda	Jefe de Infraestructura de TI

2) Equipo de Respuesta ante Incidentes de Operaciones.

   El equipo de respuesta ante incidente de Operaciones está compuesto por 4 áreas:

Tabla 39 Equipo de respuesta de redes.

ROL	INTEGRANTE	SUPLENTE 1	SUPLENTE 2
Líder del Equipo	Director de operaciones	Gerente de redes	Jefe de ingeniería y Core

Integrantes del equipo	Jefe de ingeniería y Core	Jefe NOC	Jefe de ICU
	Especialista NOC	Analista NOC 1	Analista NOC 2
	Especialista de Ingeniería	Analista de ingeniería 1	Analista de ingeniería 2
	Especialista de Core	Analista de Core	Especialista NOC
	Jefe TAC	Analista TAC 1	Analista TAC 2

Tabla 40 Equipo de respuesta de Datacenter y Nodos

ROL	INTEGRANTE	SUPLENTE 1	SUPLENTE 2
Líder del Equipo	Director de operaciones	Gerente de Datacenter y nodos	Jefe de infraestructura de red
Integrantes del equipo	Gerente de Datacenter y nodos	Jefe de infraestructura de red	
	Supervisor de infraestructura	Analista de infraestructura 1	Analista de infraestructura 1
	Supervisor de energía y mantenimiento	Analista de energía y mantenimiento	Analista de energía y mantenimiento
	Supervisor de control y seguridad	Analista de control y seguridad 1	Analista de control y seguridad 2

Tabla 41 Equipo de respuesta de Infraestructura

ROL	INTEGRANTE	SUPLENTE 1	SUPLENTE 2
Líder del Equipo	Director de operaciones	Gerente de Infraestructura y Planta externa	
Integrantes del equipo	Jefe de mantenimiento y planta externa	Jefe de emergencia	
	Supervisor de mantenimiento	Analista de mantenimiento 1	Analista de mantenimiento 2
	Supervisor de emergencias	Analista de emergencias 1	Analista de emergencias 2
	Supervisor de Obras civiles	Analista de Obras civiles 1	Analista de Obras civiles 2

Tabla 42 Equipo de respuesta de Infraestructura de TI

ROL	INTEGRANTE	SUPLENTE 1	SUPLENTE 2
Líder del Equipo	Gerente TI	Jefe de TI	Jefe de MDA
Integrantes del equipo	Jefe de TI	Jefe de MDA	Jefe de investigación TI
	Especialista TI	Analista TI 1	Analista TI 2
	Jefe de MDA	Analista de MDA 1	Analista de MDA 2
	Jefe de investigación TI	Analista de investigación TI 1	Analista de investigación TI 2

Responsabilidades:

a) Antes del evento

- Proveer de liderazgo en el desarrollo y mantenimiento del DRP
- Conocer y comprender el DRP.

- Documentar y actualizar los manuales, diagramas, procedimientos y cualquier otro documento que sea valioso para funcionamiento de las operaciones.
- Liderar y participar en los simulacros y pruebas de DRP
- Asegurar que los sistemas de contingencia estén correctamente implementados y funcionen.
- Asegurar la ejecución de las pruebas según los cronogramas establecidos.
- Documentar y actualizar el DRP.

b) Durante del evento

- Evaluar el impacto de los daños a los procesos de negocio.
- Evaluar los daños en la infraestructura de red y recursos de TI.
- Notificar y reunir a los equipos de recuperación.
- Asegurar que los equipos de recuperación estén realizando sus funciones.
- Coordinar y asegurar la disponibilidad de la infraestructura de red y los recursos de TI.
- Proveer el soporte a los usuarios y a las operaciones de Negocio durante el tiempo que dure la contingencia.
- Evaluar los daños a los equipos e infraestructura del Data Center e informarlo al equipo de comunicaciones.
- Revisar, aprobar y supervisar cualquier reemplazo y/o reparación de las instalaciones dañadas.
- Estudiar y evaluar el alcance del desastre en cada área.
- Ejecutar las actividades de recuperación según el nivel de prioridad establecido.
- Coordinar las actividades de retorno a las instalaciones de la organización.

c) Después del evento

- Evaluar la efectividad del plan de recuperación de Desastres.
- Identificar las oportunidades de mejora del DRP.
- Revisar y actualizar los procedimientos existentes, modificando las tareas y procedimientos del equipo de trabajo según sea necesario.
- Evaluar el desempeño general de los equipos de trabajo durante el proceso de activación del Plan de Continuidad del Negocio.
- Realizar la actualización del DRP en caso haber surgido modificaciones durante la situación de emergencia.

3) Equipo de respuesta comunicaciones, legal y capital humano.

Tabla 43 Equipo de respuesta de Legal y Capital Humano

ROL	INTEGRANTE	SUPLENTE 1	SUPLENTE 2
Líder del Equipo	Director Legal	Gerente de Capital Humano	Gerente de finanzas
Integrantes del equipo	Gerente de Capital Humano	Gerente de finanzas	Gerente Legal
	Jefe de capital Humano	Analista de Capital humano 1	Analista de Capital humano 2
	Gerente Legal	Personal de área Legal 1	Personal de área Legal 2
	Gerente de finanzas	Personal de finanzas 1	Personal de finanzas 2
	Jefe de SSGG y seguridad	Personal de SSGG 1	Personal de SSGG 2

Tabla 44 Equipo de respuesta de comunicaciones e imagen

ROL	INTEGRANTE	SUPLENTE 1	SUPLENTE 2
Líder del Equipo	Gerente general	Director comercial	Director de Operaciones
Integrantes del equipo	Gerente general	Director comercial	Director de Operaciones
	Jefe de marketing	Analista de marketing	Analista de marketing

a) Antes del evento

- Conocer y comprender el DRP.
- Mantener y actualizar los canales de comunicación con los medios internos, externos y las partes interesadas.

b) Durante el evento

- Asegurar la correcta comunicación del impacto del incidente disruptivo al personal y a las partes interesadas.
- Coordinar con los líderes de equipo la información que se entregará a los medios de comunicación.
- Ser el único canal autorizado y punto de contacto con los medios externos y partes interesadas durante la contingencia y a lo largo del ciclo de vida del incidente.

c) Después el evento

- Revisar y actualizar los procedimientos existentes en cuanto a comunicaciones y flujos de aprobación.
- Ser el único canal autorizado y punto de contacto con los medios internos, externos y grupos de interés a fin de informar los resultados de la crisis, continuidad del negocio y la reanudación de las actividades normales.

4.10 Árbol de comunicaciones

En la siguiente tabla se encuentra el árbol de comunicaciones, el cual será utilizado para comunicar a cada equipo de respuesta la declaratoria de emergencia.

Tabla 45 Árbol de comunicaciones

	ROL	CARGO	CELULAR
1	Contacto de Emergencia Primario para todas las áreas de negocio	Gerente General	9942xxxxx
2	Nivel 1	Director Comercial	9964 xxxxx
3	Nivel 2	Director de Operaciones	9451 xxxxx
4	Colaborador	Gerente de Data Center y Nodos	9776 xxxxx
5	Colaborador	Gerente de Operación del Servicio	9509 xxxxx
6	Colaborador	Gerente de TI	9776 xxxxx
7	Colaborador	Gerente de Redes	9231 xxxxx
8	Colaborador	Jefe NOC	9955 xxxxx
9	Colaborador	Analista NOC	9553 xxxxx
10	Colaborador	Especialista NOC	9554 xxxxx
11	Colaborador	Jefe de ingeniería y Core	9555 xxxxx
12	Colaborador	Jefe TAC	9556 xxxxx
13	Colaborador	Jefe de infraestructura de red	9557 xxxxx
14	Colaborador	Supervisor de infraestructura	9558 xxxxx
15	Colaborador	Analista de infraestructura	9559 xxxxx
16	Colaborador	Supervisor de energía y mantenimiento	9560 xxxxx
17	Colaborador	Supervisor de control y seguridad	9561 xxxxx
18	Colaborador	Jefe de mantenimiento y planta externa	9562 xxxxx
19	Colaborador	Supervisor de emergencias	9563 xxxxx
20	Colaborador	Supervisor de Obras civiles	9564 xxxxx
21	Colaborador	Jefe de TI	9565 xxxxx
22	Colaborador	Especialista TI	9566 xxxxx
23	Colaborador	Jefe de MDA	9567 xxxxx
24	Colaborador	Jefe de investigación TI	9568 xxxxx
25	Colaborador	Director Legal	9579 xxxxx
26	Colaborador	Jefe de capital Humano	9540 xxxxx
27	Colaborador	Gerente Legal	9571 xxxxx
28	Colaborador	Gerente de finanzas	9572 xxxxx
29	Colaborador	Jefe de SSGG y seguridad	9573 xxxxx
30	Colaborador	Jefe de marketing	9574 xxxxx

4.11 Actividades de prueba, ejercicio y entrenamiento TT&E

4.11.1 Escenario de prueba: Falla de DC principal

Pruebas de redundancia de equipos Core:

Escenario:

Los equipos de Core que están alojados tanto en el datacenter principal y de respaldo están virtualizados con un protocolo de Cisco llamado VSS, lo cual hace que los equipos trabajen como una sola unidad lógica, sin embargo, el sistema tiene los roles de Active y Standby, siendo el rol Active quien realiza todas las tareas de procesamiento y control del sistema.

Objetivo:

El propósito de esta esta prueba es simular la afectación de los equipos Core del datacenter principal (krumdick) y demostrar que el datacenter Alterno es capaz de asumir el rol de principal y permitir la continuidad de las operaciones

Lugar y Fecha:

El ejercicio se realizó en la ciudad de Lima en el distrito San Borja y La victoria simultáneamente el día 28 de julio del año 2019 de hora 00:00 a 04:00 -5GMT

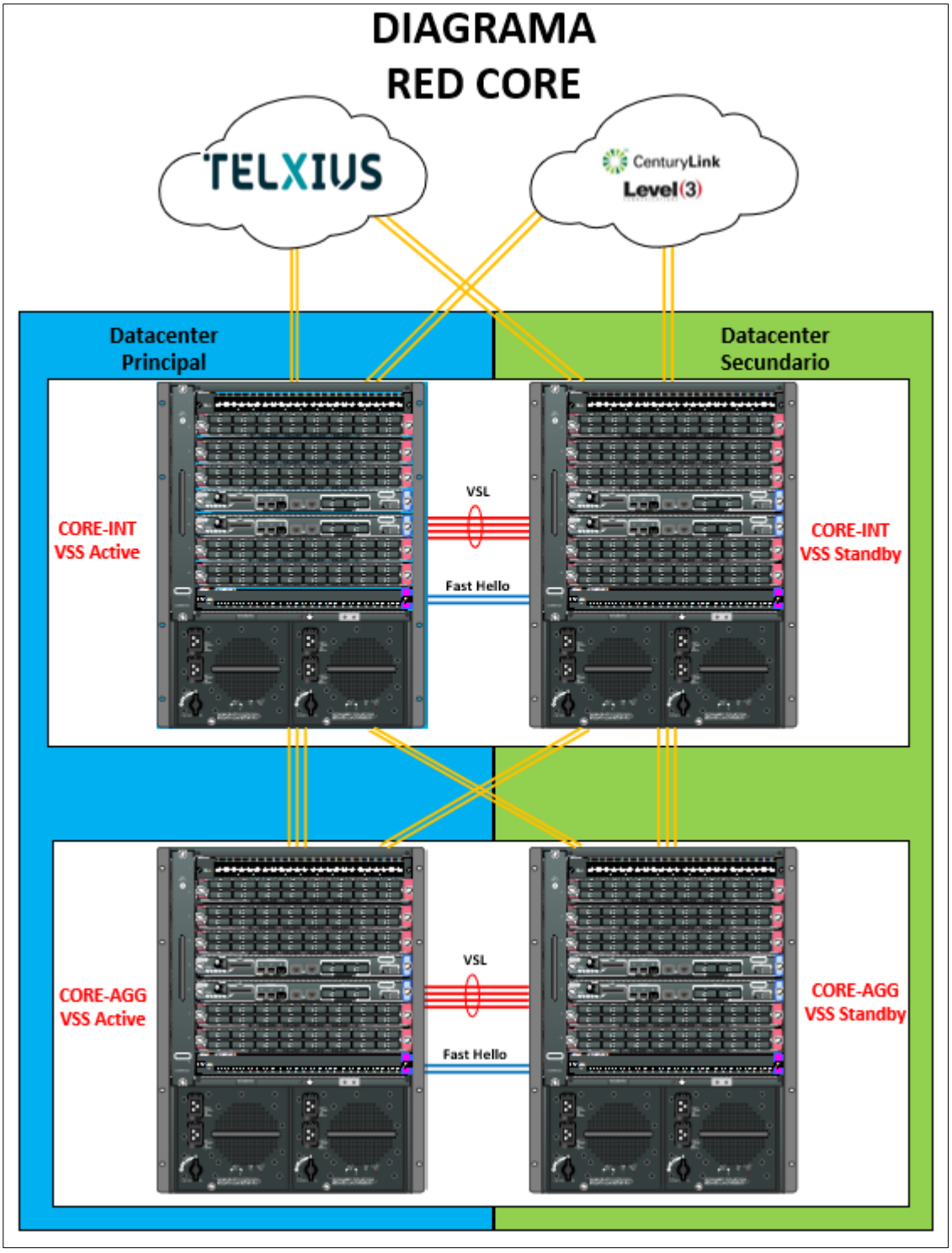


Figura 14 Diagrama de equipos CORE

Fuente: Elaboración propia

4.11.1.1 Simulación de falla de equipos Core-INT

Escenarios de desastre:

- Incendio que afecta local del Data Center principal (DC1).
- Inundación que afecta el Local del Data Center Principal (DC1).
- Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1).
- Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias.

Proceso de negocio afectado:

- Internet

Prueba 1: conmutación de roles equipo Core-INT

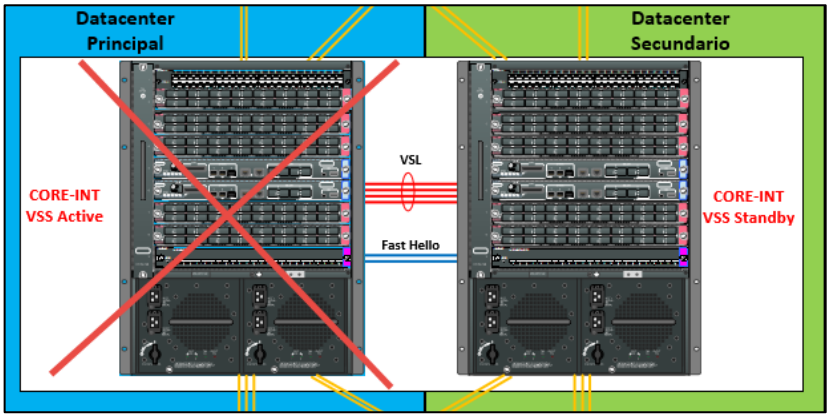


Figura 15 Simulación de falla Equipo Core-INT 1
Fuente: elaboración propia.

Verificaciones previas:

Antes de realizar el cambio se puede observar que el equipo de Core-Int Krumdieck tiene el role de activo:

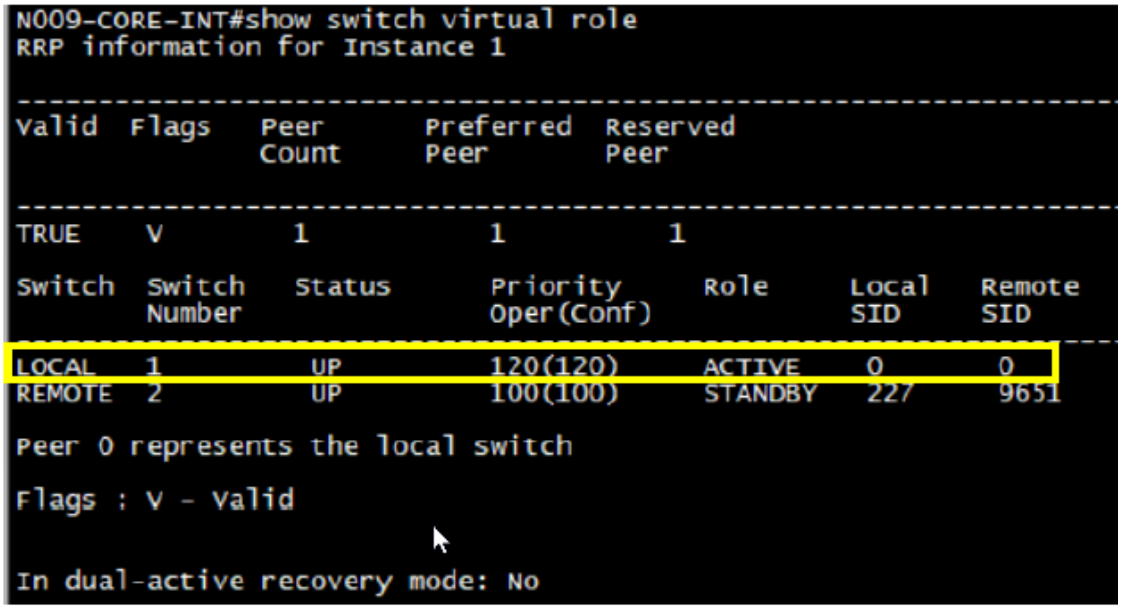


Figura 16 Verificación de role Router Core-INT

Antes de realizar la conmutación se observa que supervisora mantiene el role de activo y cuál será la supervisora que asumirá el role después de la conmutación.

El numero 1 indica que el switch 1 (DC Krumdieck) modulo 5 es la supervisora activa
El numero 2 indica que el switch 2 (DC Gálvez) modulo 5 será la siguiente supervisora active ante una conmutación de role.

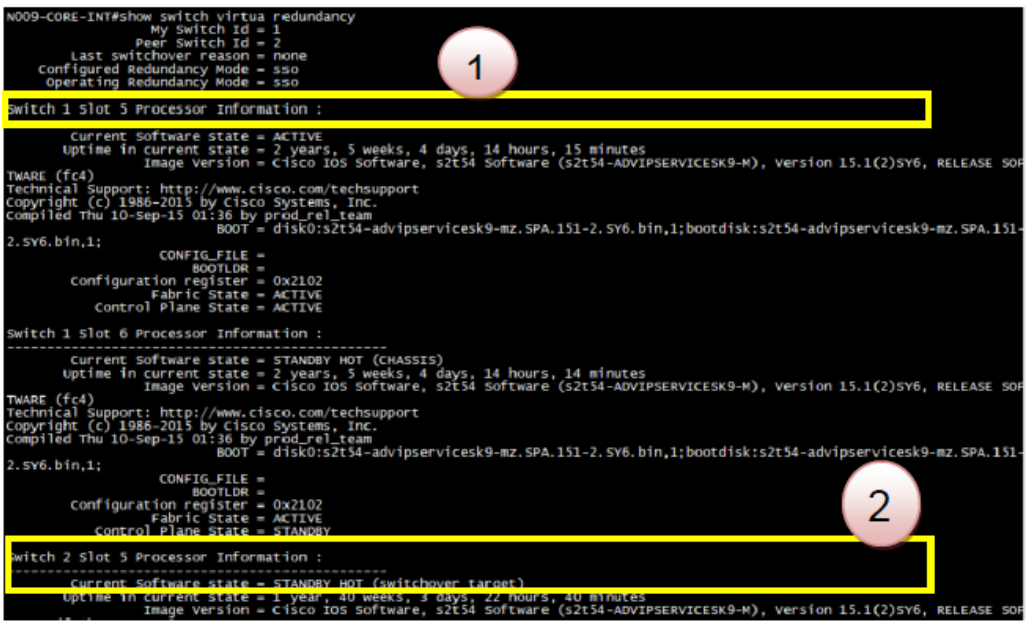


Figura 17 Verificación de secuencia de conmutación de roles.

Al realizar el cambio el de role mediante el comando “redundancy force-switchover” el módulo 5 del switch 1 (Nodo Krumdieck) se reiniciará y se procederá con el cambio y observemos los resultados:

Captura consola del módulo 5 switch 1 (Nodo Krumdieck) Reiniciándose

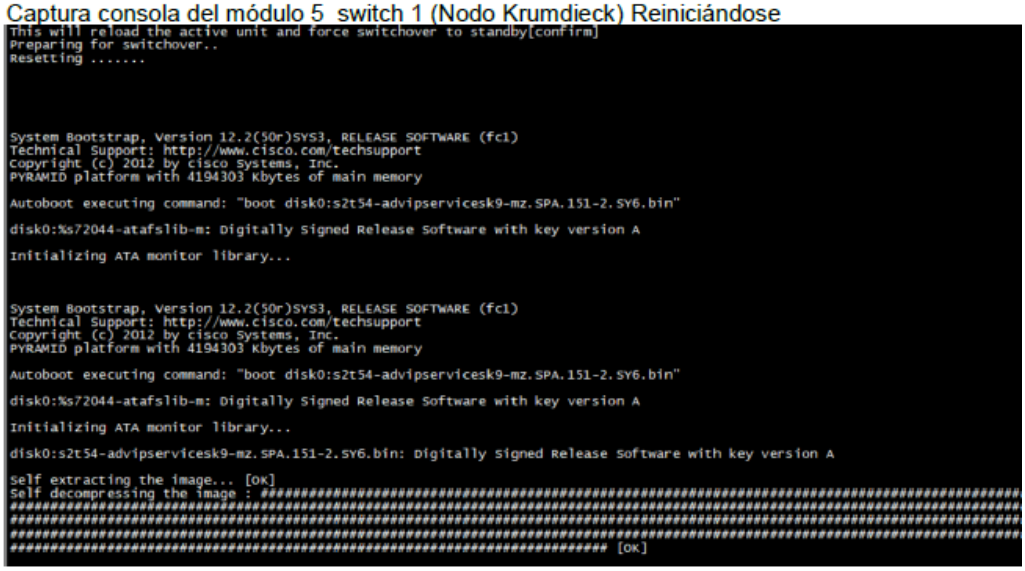


Figura 18 Proceso de reinicio del módulo 5 vss 1

Observamos el nuevo equipo activo switch ID 2 (DC Gálvez)

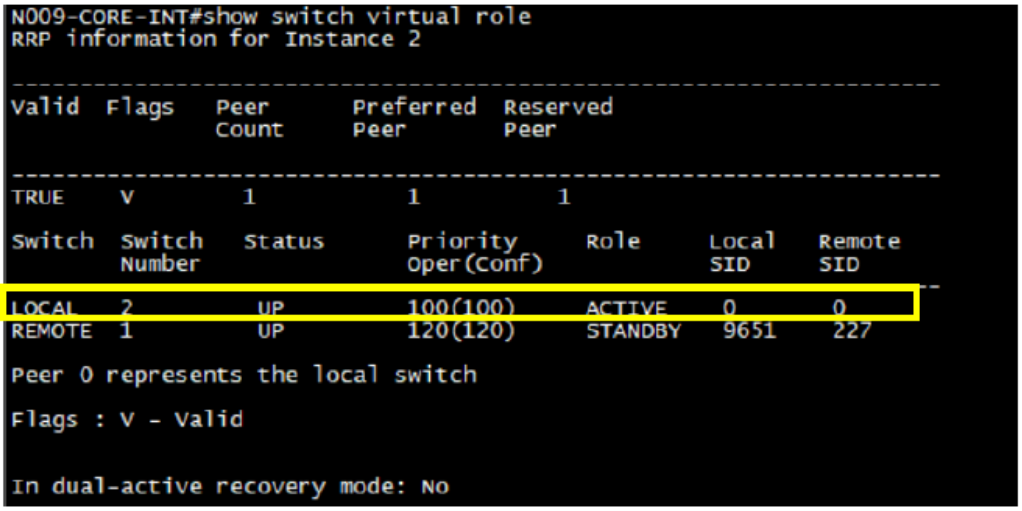


Figura 19 Comprobación de roles del sistema VSS

El numero 1 indica que el switch 2 (DC Gálvez) modulo 5 asumió el role de supervisora activa

El numero 2 indica que el switch 1 (DC Krumdieck) modulo 6 será la siguiente supervisora active ante una conmutación de role

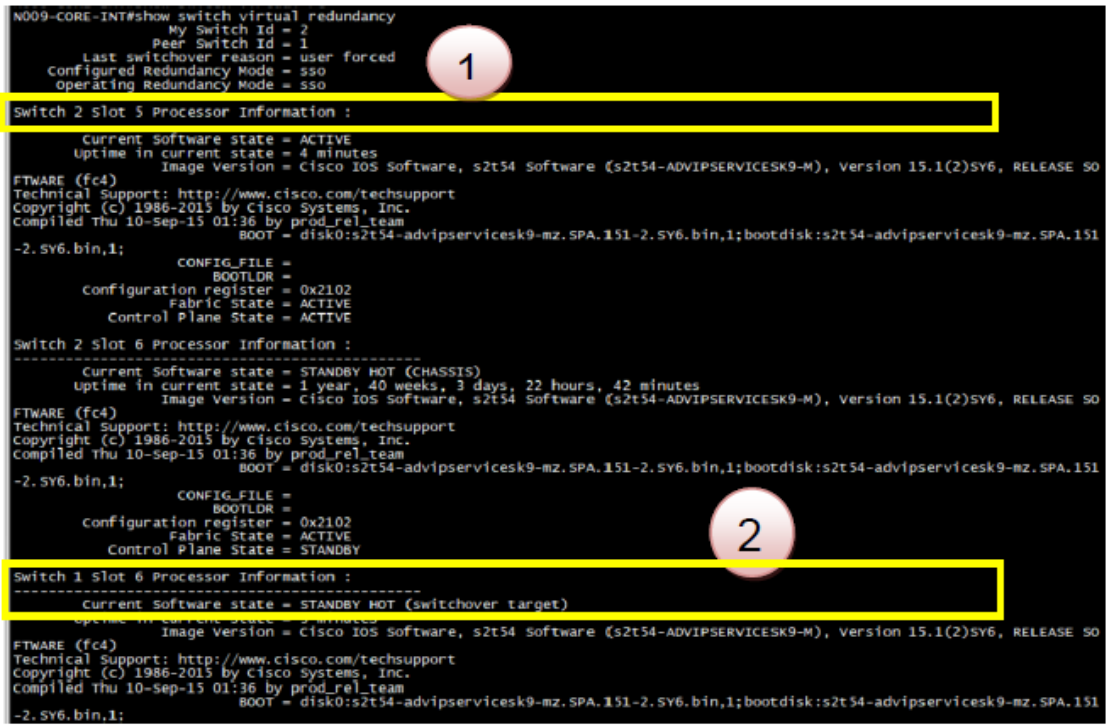


Figura 20 Validación de secuencia de cambio de roles

Prueba 2: Apagado de tarjetas Core-INT.

Verificación: Antes de realizar la prueba se puede observar que el equipo de Core-INT Krumdieck tiene todos los módulos encendidos.

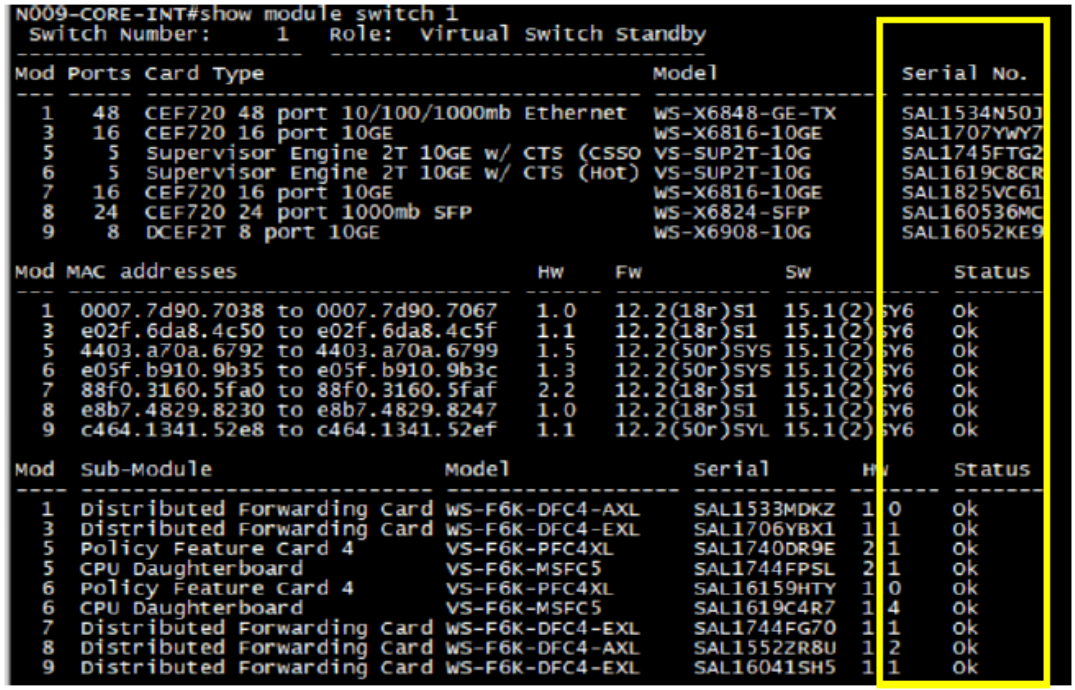


Figura 21 Validación de tarjetas encendidas

Se procede a apagar las tarjetas del switch Core-INT alojado en el DC1 Verificación de módulos apagados solo las supervisoras se mantienen activas

```
N009-CORE-INT#show module switch 1
 Switch Number:     1   Role:  Virtual Switch Standby
---------------------  ---------------------------
Mod Ports Card Type                                 Model              Serial No.
--- ----- ----------------------------------------- ------------------ -----------
  1    48  CEF720 48 port 10/100/1000mb Ethernet    WS-X6848-GE-TX     SAL1534N50J
  3    16  CEF720 16 port 10GE                       WS-X6816-10GE      SAL1707YWY7
  5     5  Supervisor Engine 2T 10GE w/ CTS (CSSO    VS-SUP2T-10G       SAL1745FTG2
  6     5  Supervisor Engine 2T 10GE w/ CTS (Hot)    VS-SUP2T-10G       SAL1619C8CR
  7    16  CEF720 16 port 10GE                       WS-X6816-10GE      SAL1825VC61
  8    24  CEF720 24 port 1000mb SFP                 WS-X6824-SFP       SAL160536MC
  9     8  DCEF2T 8 port 10GE                        WS-X6908-10G       SAL16052KE9

Mod MAC addresses                          Hw     Fw           Sw           Status
--- ------------------------------------- ------ ------------ ------------ -------
  1  0007.7d90.7038 to 0007.7d90.7067   1.0    12.2(18r)S1  15.1(2)SY6   PwrDown
  3  e02f.6da8.4c50 to e02f.6da8.4c5f   1.1    12.2(18r)S1  15.1(2)SY6   PwrDown
  5  4403.a70a.6792 to 4403.a70a.6799   1.5    12.2(50r)SYS 15.1(2)SY6   Ok
  6  e05f.b910.9b35 to e05f.b910.9b3c   1.3    12.2(50r)SYS 15.1(2)SY6   Ok
  7  88f0.3160.5fa0 to 88f0.3160.5faf   2.2    12.2(18r)S1  15.1(2)SY6   PwrDown
  8  e8b7.4829.8230 to e8b7.4829.8247   1.0    12.2(18r)S1  15.1(2)SY6   PwrDown
  9  c464.1341.52e8 to c464.1341.52ef   1.1    12.2(50r)SYL 15.1(2)SY6   PwrDown

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------ -------
  1  Distributed Forwarding Card WS-F6K-DFC4-AXL    SAL1533MDKZ  1.0    PwrDown
  3  Distributed Forwarding Card WS-F6K-DFC4-EXL    SAL1706YBX1  1.1    PwrDown
  5  Policy Feature Card 4       VS-F6K-PFC4XL      SAL1740DR9E  2.1    Ok
  5  CPU Daughterboard           VS-F6K-MSFC5       SAL1744FPSL  2.1    Ok
  6  Policy Feature Card 4       VS-F6K-PFC4XL      SAL16159HTY  1.0    Ok
  6  CPU Daughterboard           VS-F6K-MSFC5       SAL1619C4R7  1.4    Ok
  7  Distributed Forwarding Card WS-F6K-DFC4-EXL    SAL1744FG70  1.1    PwrDown
  8  Distributed Forwarding Card WS-F6K-DFC4-AXL    SAL1552ZR8U  1.2    PwrDown
  9  Distributed Forwarding Card WS-F6K-DFC4-EXL    SAL16041SH5  1.1    PwrDown

Mod  Online Diag Status
---- --------------------
  1  Not Applicable
  3  Not Applicable
  5  Pass
  6  Pass
  7  Not Applicable
  8  Not Applicable
  9  Not Applicable
```

Resultados:

Figura 22 Verificación de tarjetas apagadas

Una vez realizado el apagado de las tarjetas en el equipo principal se observa como el tráfico hacia el proveedor Level 3 es conmutado por el enlace de respaldo de manera automática.

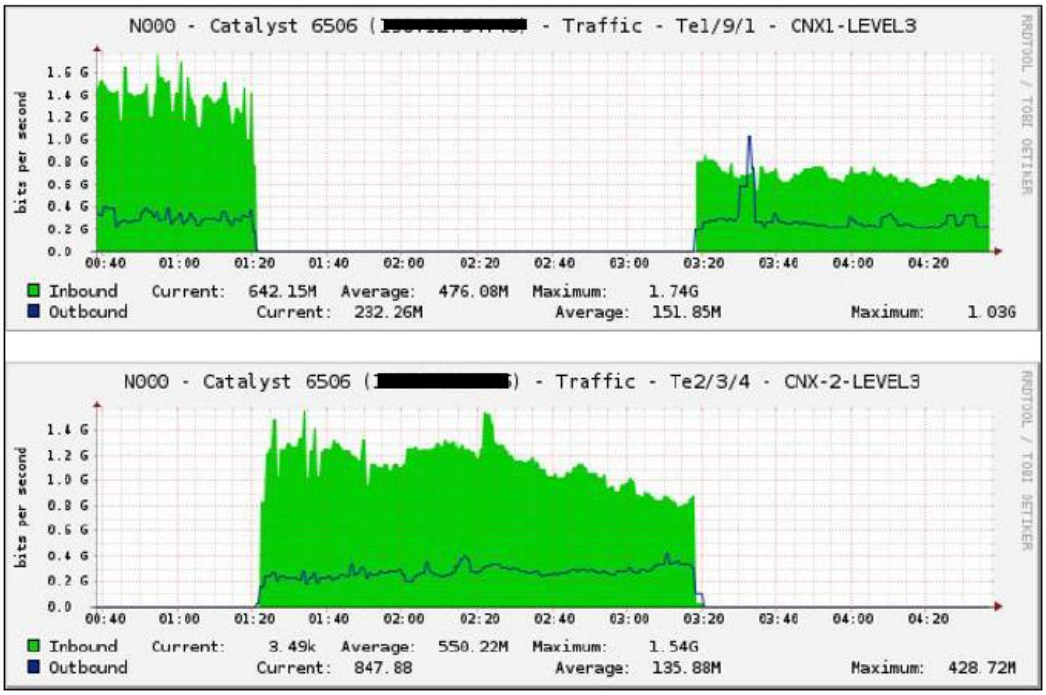


Figura 23 Validación de conmutación de tráfico del proveedor Level 3

Se verifica que el tráfico hacia el proveedor Telxius también conmuta de manera automática.

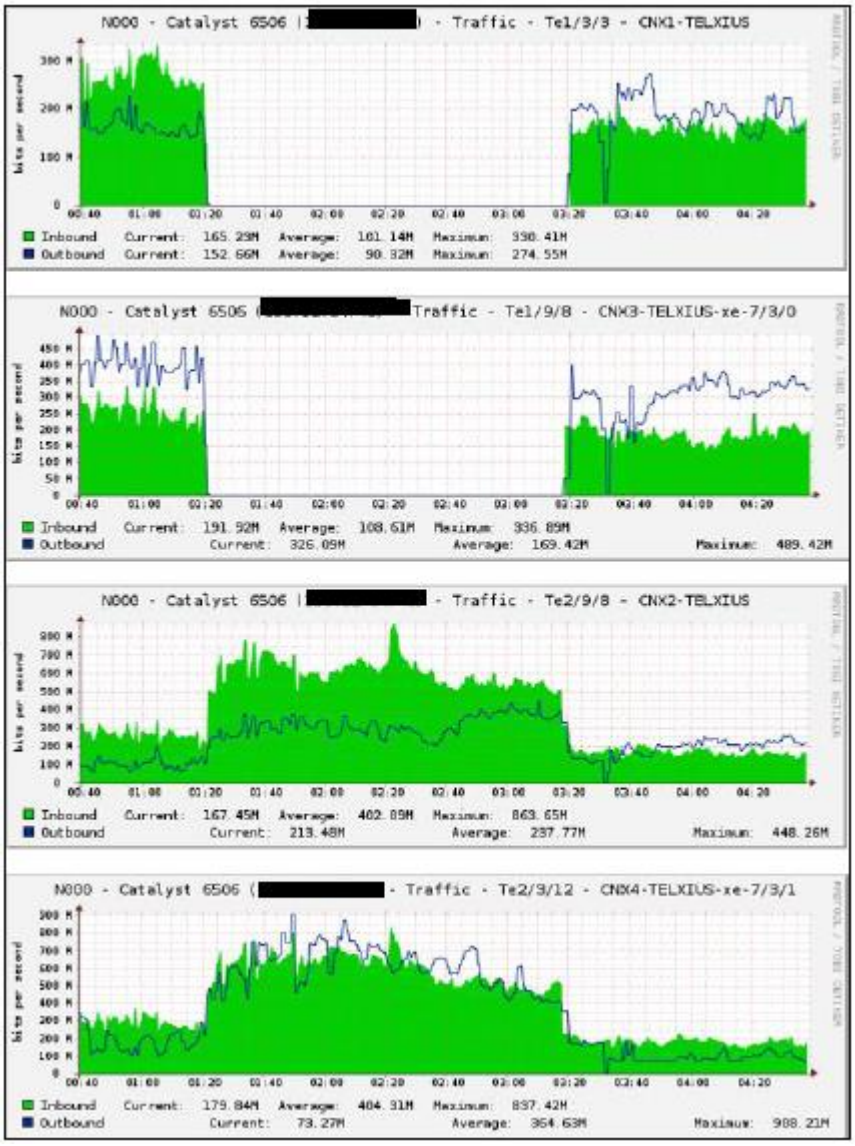


Figura 24 Validación de conmutación de tráfico del proveedor Telxius

4.11.1.2 Simulación de falla de equipos Core-AGG

Escenarios de desastre:

- Incendio que afecta local del Data Center principal (DC1).
- Inundación que afecta el Local del Data Center Principal (DC1).
- Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1).
- Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias.

Proceso de negocio afectado:

- Internet
- Interconexión de sedes
- Servicios gestionados
- Telefonía
- Servicios en la nube
- Servicios adicionales
- Centro de datos
- Lan Center
- Streaming

Prueba 1: conmutación de roles equipo Core-AGG

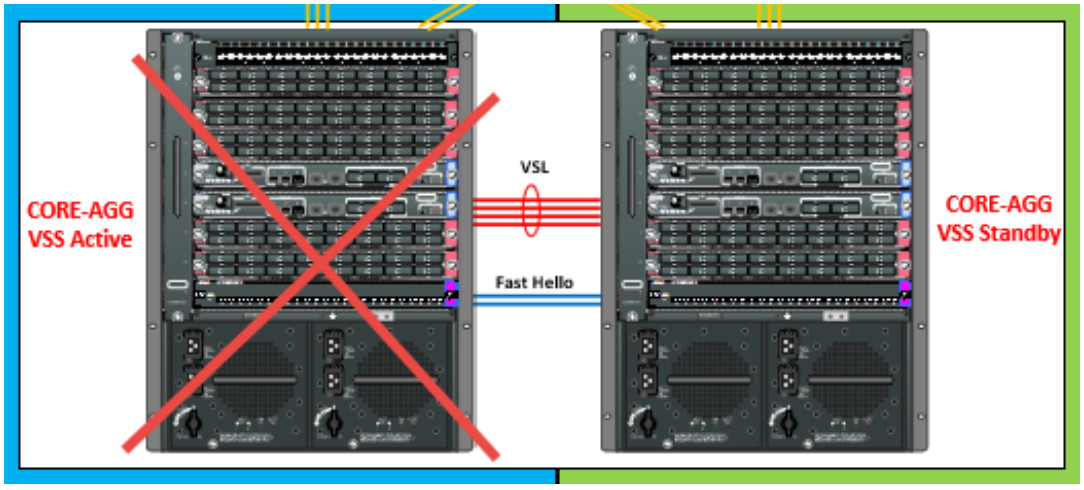


Figura 25 Diagrama de escenario de falla Core-AGG

Antes de realizar la prueba se puede observar que el equipo de Core-AGG Krumdieck tiene el role de activo:

```
N009-AGREGACION-VSS#SHOw Switch VIrtual ROle
RRP information for Instance 1

-------------------------------------------------------------------
Valid  Flags   Peer       Preferred  Reserved
               Count      Peer       Peer

-------------------------------------------------------------------
TRUE    V        1          1          1

Switch  Switch   Status     Priority     Role     Local    Remote
        Number              Oper(Conf)            SID      SID
-------------------------------------------------------------------
LOCAL   1         UP        110(110)     ACTIVE   0        0
REMOTE  2         UP        100(100)     STANDBY  1707     1570

Peer 0 represents the local switch

Flags : V - Valid


In dual-active recovery mode: No
```

Figura 26 Validación de roles del sistema VSS Core-Agg

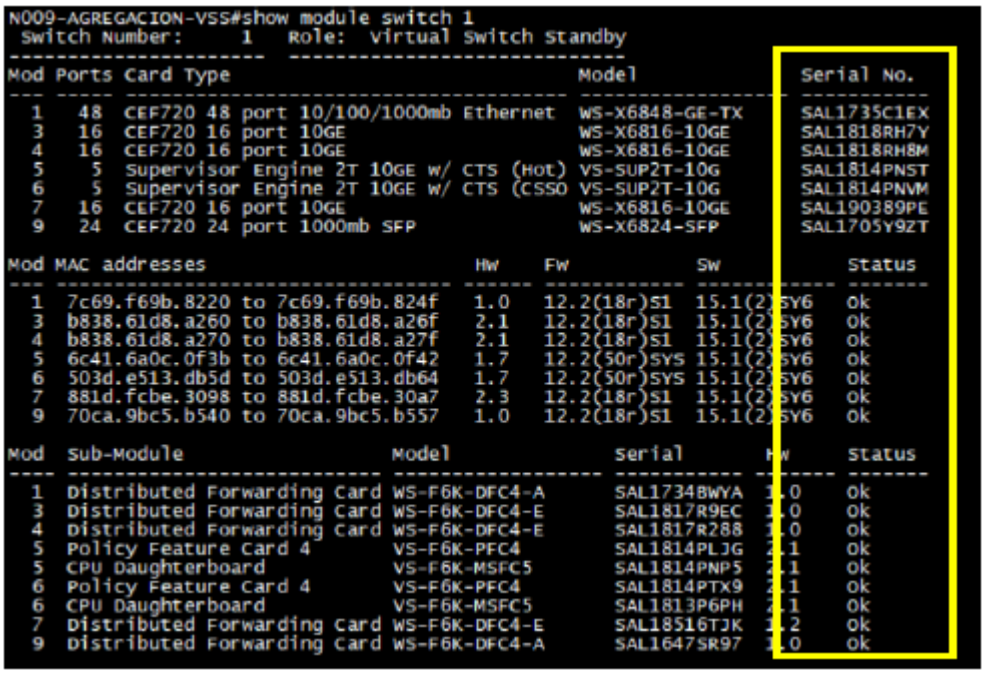
Al realizar el cambio el de role mediante el comando “redundancy force-switchover” el módulo 5 del switch 1 (Nodo Krumdieck) se reiniciará y se procederá con el cambio y observemos que el nuevo equipo activo switch ID 2 (DC Gálvez)

```
N009-AGREGACION-VSS#show switch virtual role
RRP information for Instance 2

-------------------------------------------------------------------
Valid  Flags   Peer       Preferred  Reserved
               Count      Peer       Peer

-------------------------------------------------------------------
TRUE    V        1          1          1

Switch  Switch   Status     Priority     Role     Local    Remote
        Number              Oper(Conf)            SID      SID
-------------------------------------------------------------------
LOCAL   2         UP        100(100)     ACTIVE   0        0
REMOTE  1         UP        110(110)     STANDBY  5235     8573

Peer 0 represents the local switch

Flags : V - Valid


In dual-active recovery mode: No
```

Figura 27 Validación de cambio de roles Core-Agg

Prueba 2: Apagado de tarjetas Core-AGG.

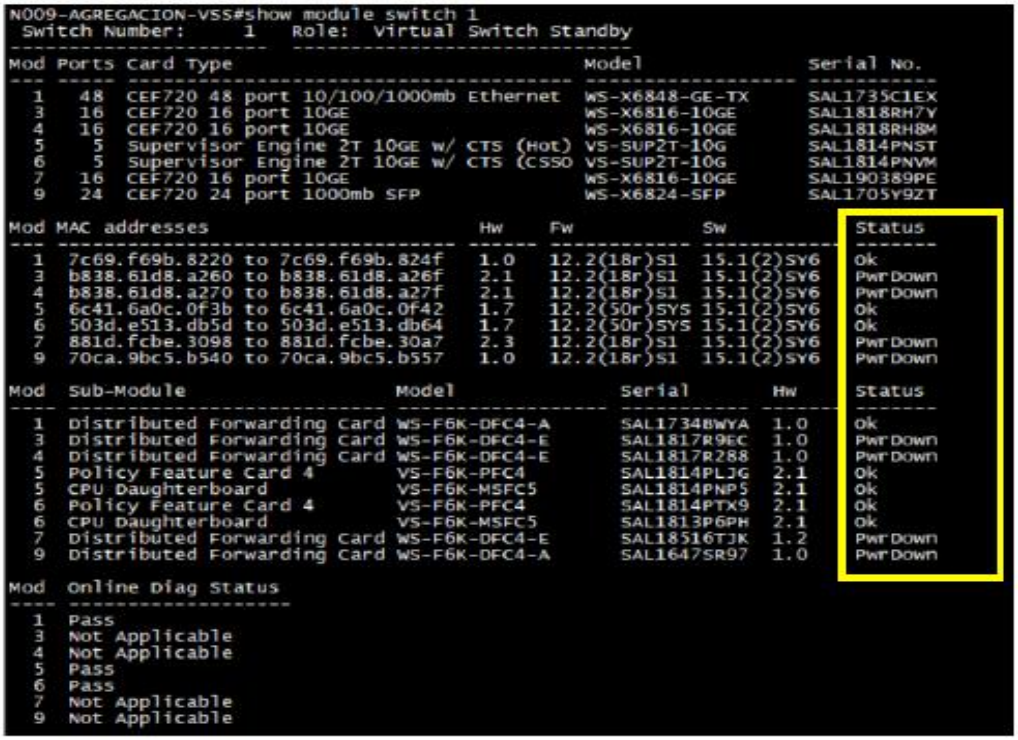
Verificación: Antes de realizar se valida que todas las tarjetas del switch Core-AGG se encuentran activas.



```
N009-AGREGACION-VSS#show module switch 1
 Switch Number:     1   Role:  Virtual Switch Standby
---------------------  ---------------------------
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  1    48  CEF720 48 port 10/100/1000mb Ethernet  WS-X6848-GE-TX     SAL1735C1EX
  3    16  CEF720 16 port 10GE                    WS-X6816-10GE      SAL1818RH7Y
  4    16  CEF720 16 port 10GE                    WS-X6816-10GE      SAL1818RH8M
  5     5  Supervisor Engine 2T 10GE w/ CTS (Hot) VS-SUP2T-10G       SAL1814PNST
  6     5  Supervisor Engine 2T 10GE w/ CTS (CSSO VS-SUP2T-10G       SAL1814PNVM
  7    16  CEF720 16 port 10GE                    WS-X6816-10GE      SAL190389PE
  9    24  CEF720 24 port 1000mb SFP              WS-X6824-SFP       SAL1705Y9ZT

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  7c69.f69b.8220 to 7c69.f69b.824f   1.0    12.2(18r)S1  15.1(2)SY6   Ok
  3  b838.61d8.a260 to b838.61d8.a26f   2.1    12.2(18r)S1  15.1(2)SY6   Ok
  4  b838.61d8.a270 to b838.61d8.a27f   2.1    12.2(18r)S1  15.1(2)SY6   Ok
  5  6c41.6a0c.0f3b to 6c41.6a0c.0f42   1.7    12.2(50r)SYS 15.1(2)SY6   Ok
  6  503d.e513.db5d to 503d.e513.db64   1.7    12.2(50r)SYS 15.1(2)SY6   Ok
  7  881d.fcbe.3098 to 881d.fcbe.30a7   2.3    12.2(18r)S1  15.1(2)SY6   Ok
  9  70ca.9bc5.b540 to 70ca.9bc5.b557   1.0    12.2(18r)S1  15.1(2)SY6   Ok

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ------------ ------ -------
  1  Distributed Forwarding Card WS-F6K-DFC4-A      SAL1734BWYA  1.0    Ok
  3  Distributed Forwarding Card WS-F6K-DFC4-E      SAL1817R9EC  1.0    Ok
  4  Distributed Forwarding Card WS-F6K-DFC4-E      SAL1817R288  1.0    Ok
  5  Policy Feature Card 4       VS-F6K-PFC4        SAL1814PLJG  2.1    Ok
  5  CPU Daughterboard           VS-F6K-MSFC5       SAL1814PNP5  2.1    Ok
  6  Policy Feature Card 4       VS-F6K-PFC4        SAL1814PTX9  2.1    Ok
  6  CPU Daughterboard           VS-F6K-MSFC5       SAL1813P6PH  2.1    Ok
  7  Distributed Forwarding Card WS-F6K-DFC4-E      SAL18516TJK  1.2    Ok
  9  Distributed Forwarding Card WS-F6K-DFC4-A      SAL1647SR97  1.0    Ok
```

Figura 28 Verificación de tarjetas encendidas Core-Agg

Se procede a apagar las tarjetas del switch Core-AGG alojado en el DC1



```
N009-AGREGACION-VSS#show module switch 1
 Switch Number:     1   Role:  Virtual Switch Standby
---------------------  ---------------------------
Mod Ports Card Type                                Model              Serial No.
--- ----- ---------------------------------------- ------------------ -----------
  1    48  CEF720 48 port 10/100/1000mb Ethernet  WS-X6848-GE-TX     SAL1735C1EX
  3    16  CEF720 16 port 10GE                    WS-X6816-10GE      SAL1818RH7Y
  4    16  CEF720 16 port 10GE                    WS-X6816-10GE      SAL1818RH8M
  5     5  Supervisor Engine 2T 10GE w/ CTS (Hot) VS-SUP2T-10G       SAL1814PNST
  6     5  Supervisor Engine 2T 10GE w/ CTS (CSSO VS-SUP2T-10G       SAL1814PNVM
  7    16  CEF720 16 port 10GE                    WS-X6816-10GE      SAL190389PE
  9    24  CEF720 24 port 1000mb SFP              WS-X6824-SFP       SAL1705Y9ZT

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  7c69.f69b.8220 to 7c69.f69b.824f   1.0    12.2(18r)S1  15.1(2)SY6   Ok
  3  b838.61d8.a260 to b838.61d8.a26f   2.1    12.2(18r)S1  15.1(2)SY6   Pwr Down
  4  b838.61d8.a270 to b838.61d8.a27f   2.1    12.2(18r)S1  15.1(2)SY6   Pwr Down
  5  6c41.6a0c.0f3b to 6c41.6a0c.0f42   1.7    12.2(50r)SYS 15.1(2)SY6   Ok
  6  503d.e513.db5d to 503d.e513.db64   1.7    12.2(50r)SYS 15.1(2)SY6   Ok
  7  881d.fcbe.3098 to 881d.fcbe.30a7   2.3    12.2(18r)S1  15.1(2)SY6   Pwr Down
  9  70ca.9bc5.b540 to 70ca.9bc5.b557   1.0    12.2(18r)S1  15.1(2)SY6   Pwr Down

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ------------ ------ -------
  1  Distributed Forwarding Card WS-F6K-DFC4-A      SAL1734BWYA  1.0    Ok
  3  Distributed Forwarding Card WS-F6K-DFC4-E      SAL1817R9EC  1.0    Pwr Down
  4  Distributed Forwarding Card WS-F6K-DFC4-E      SAL1817R288  1.0    Pwr Down
  5  Policy Feature Card 4       VS-F6K-PFC4        SAL1814PLJG  2.1    Ok
  5  CPU Daughterboard           VS-F6K-MSFC5       SAL1814PNP5  2.1    Ok
  6  Policy Feature Card 4       VS-F6K-PFC4        SAL1814PTX9  2.1    Ok
  6  CPU Daughterboard           VS-F6K-MSFC5       SAL1813P6PH  2.1    Ok
  7  Distributed Forwarding Card WS-F6K-DFC4-E      SAL18516TJK  1.2    Pwr Down
  9  Distributed Forwarding Card WS-F6K-DFC4-A      SAL1647SR97  1.0    Pwr Down

Mod  Online Diag Status
---- --------------------
  1  Pass
  3  Not Applicable
  4  Not Applicable
  5  Pass
  6  Pass
  7  Not Applicable
  9  Not Applicable
```

Figura 29 Apagado de tarjetas de equipo Core-Agg

Resultados:

Una vez realizado el apagado de las tarjetas en el equipo principal se observa como el tráfico proveniente de los equipos de backbone conmutan de manera automática hacia el enlace secundario.

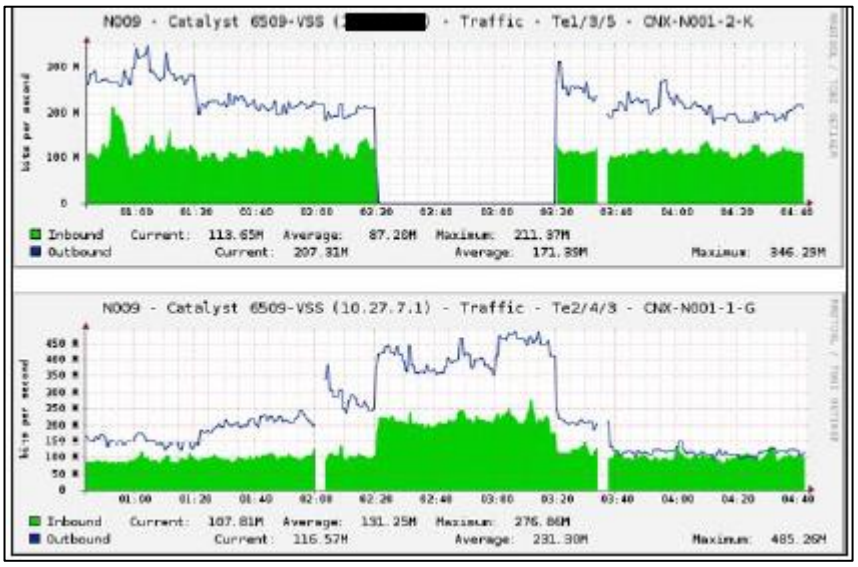


Figura 30 Validación de redundancia de tráfico para nodo N001

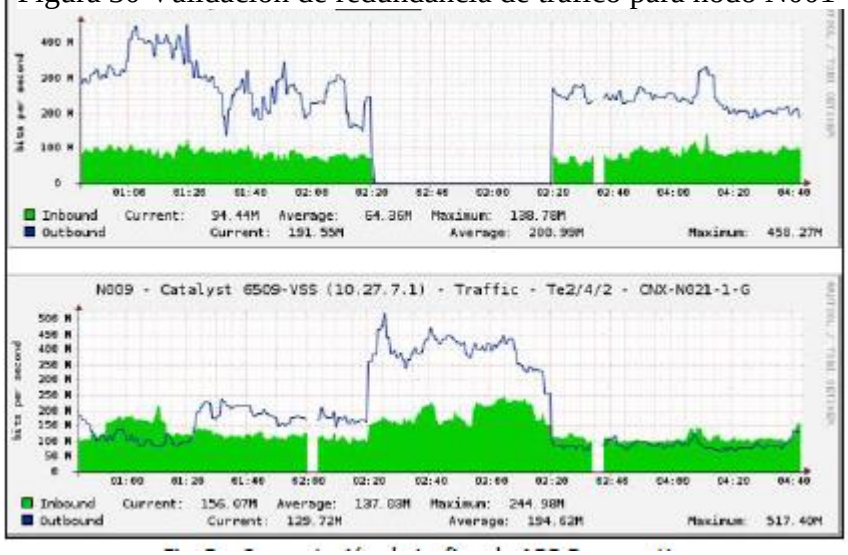


Figura 31 Validación de redundancia de tráfico para nodo N021

El trafico global de la red backbone no se afectado por la simulación de falla de los equipos alojados en el DC 1.

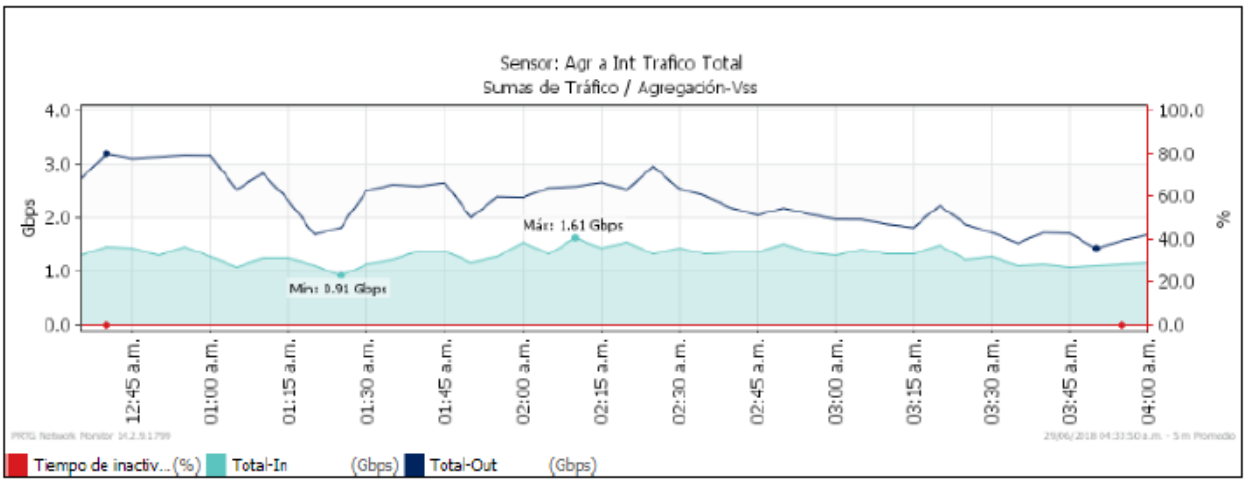


Figura 32 Verificación del tráfico global, sin afectación

Conclusiones:

- Los trabajos de prueba de redundancia en el equipo Internet VSS no tuvieron inconvenientes se dieron los comportamientos esperados a nivel de Sistema VSS, se observó que todos los servicios mantuvieron la disponibilidad ante la caída del equipo Internet Krumdieck VSS.
- Los trabajos de prueba de redundancia en el equipo Agregación VSS no tuvieron inconvenientes se dieron los comportamientos esperados a nivel de Sistema VSS, se puedo que los servicio hacia los clientes no presentaron indisponibilidad.
- Las pruebas de redundancia demostraron que los enlaces de contingencia funcionan correctamente y son capaces de soportar toda la carga de los equipos de Core del Datacenter principal.

4.11.2 Pruebas de Mitigación de ataques de tipo DDoS.

Objetivo:

El objetivo de esta prueba es comprobar la efectividad de los procedimientos y herramientas implementadas para ataques volumétricos de tipo de DDoS mayores a 20 Gbps.

Lugar y Fecha:

La prueba se realizó en la ciudad de Lima en el distrito de San Borja 31 de agosto de 2019

Escenarios de desastre:

- Ataque DDoS mayor a 20Gbps y/o por más de 10 horas.

Proceso de negocio afectado:

- Internet

Actividad 1: Detección del ataque.

La herramienta de mitigación Arbor TMS identifica un ataque dirigido a la dirección IP 161.132.98.176/32, con un impacto máximo de 44.5 Gbps/4.4 Mpps.

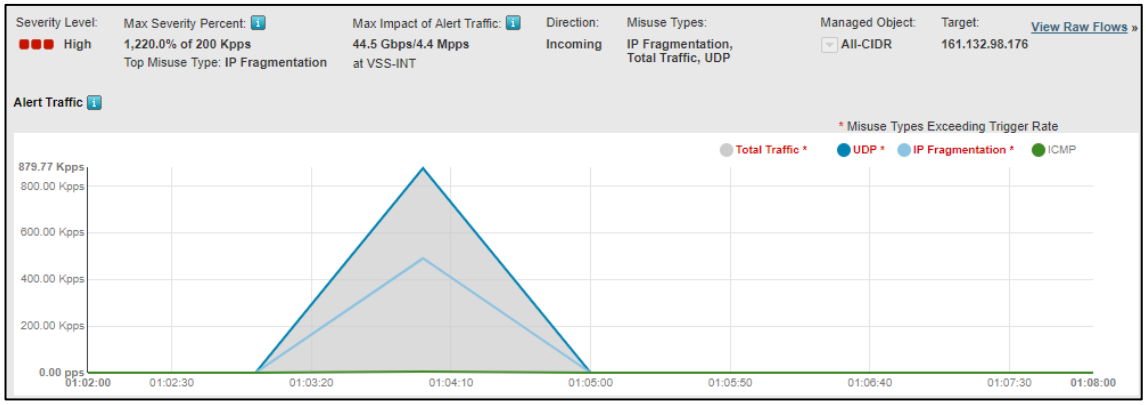


Figura 33 Detección de ataque DDoS

Actividad 2: Mitigación del ataque en la nube.

Debido a que el ataque superó los 20 Gbps la mitigación inicia de manera inmediata en la herramienta Arbor Cloud.

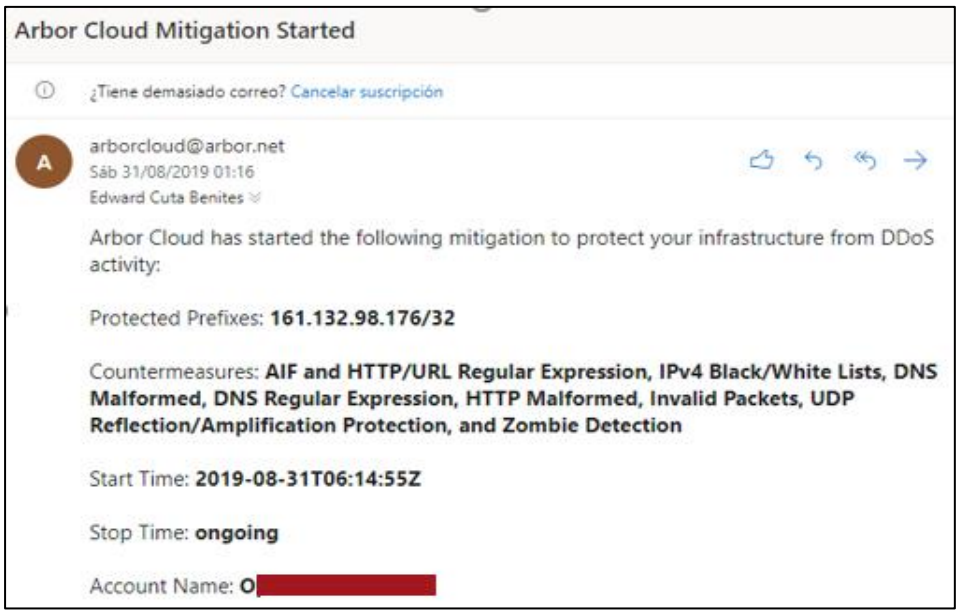


Figura 34 Notificación de mitigación Cloud

Desde el portal de Arbor Cloud se puede visualizar que el tráfico está desviado hacia la herramienta.

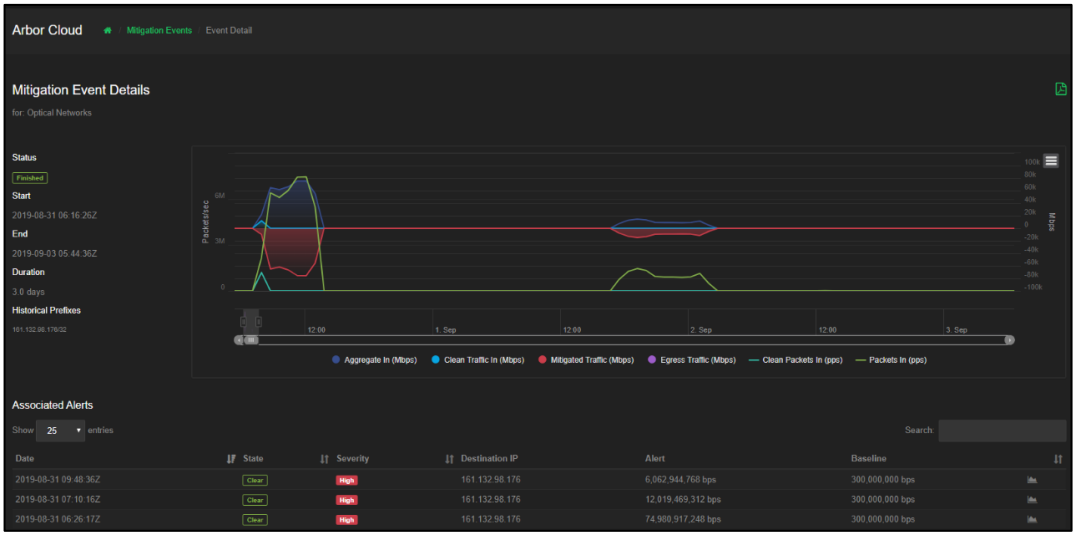


Figura 35 Consola de herramienta de mitigación Cloud

Actividad 3: Comunicación con el área TAC

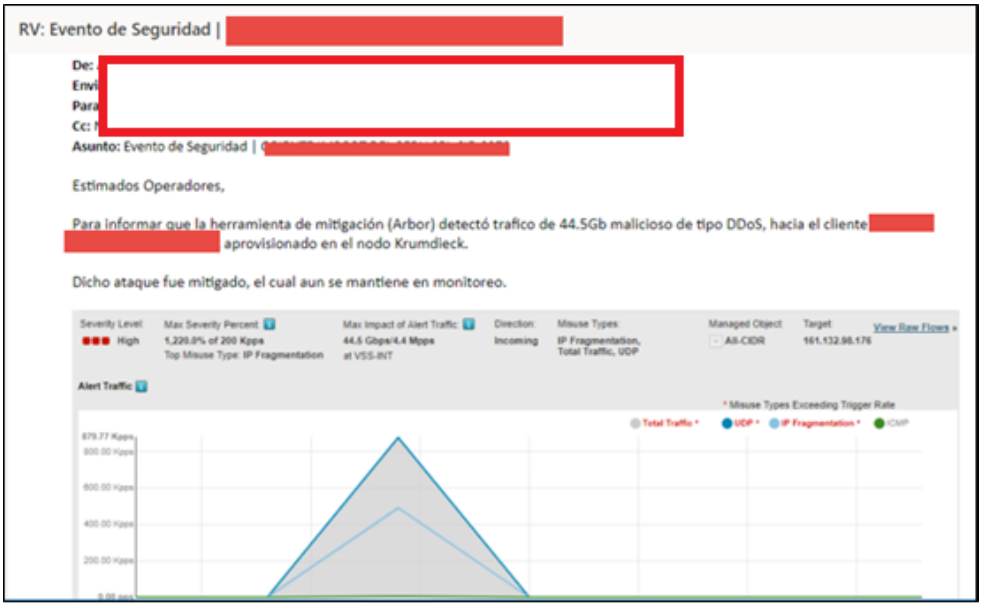


Figura 36 Notificación del evento vía correo

Actividad 4: Fin de mitigación.

Pasado las 72 horas se finaliza la mitigación en la nube.

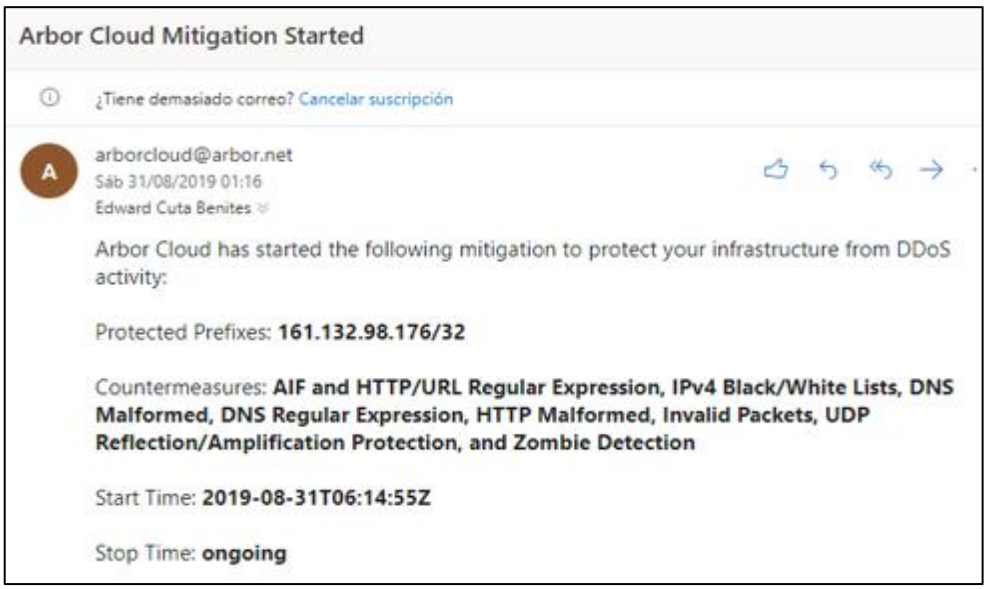


Figura 37 Notificación de fin de mitigación Cloud

Conclusiones:

- Las pruebas fueron satisfactorias, el nivel tráfico superó los 20Gbps esperados sin llegar a afectar los servicios.
- Las herramientas identificaron de manera efectiva el tráfico malicioso y activo la mitigación en la nube de manera inmediata.
- La comunicación con las áreas interesadas fue efectiva.

4.11.3 Pruebas de redundancia de proveedores de internet:

Objetivo:

El objetivo de esta prueba es comprobar la redundancia automática del servicio de internet entre los proveedores internacionales Telxius y CenturyLink (Level 3), y asegurar que cada proveedor es capaz de soportar el 100% del tráfico del otro.

Escenarios de desastre:

- Incendio que afecta local del Data Center principal (DC1).
- Inundación que afecta el Local del Data Center Principal (DC1).

- Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1).
- Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias.

Proceso de negocio afectado:

- Internet

Actividad 1: Prueba de redundancia de Level 3 (CenturyLink) a Telxius

Se desactiva el tráfico proveniente del proveedor Level 3 (CenturyLink)

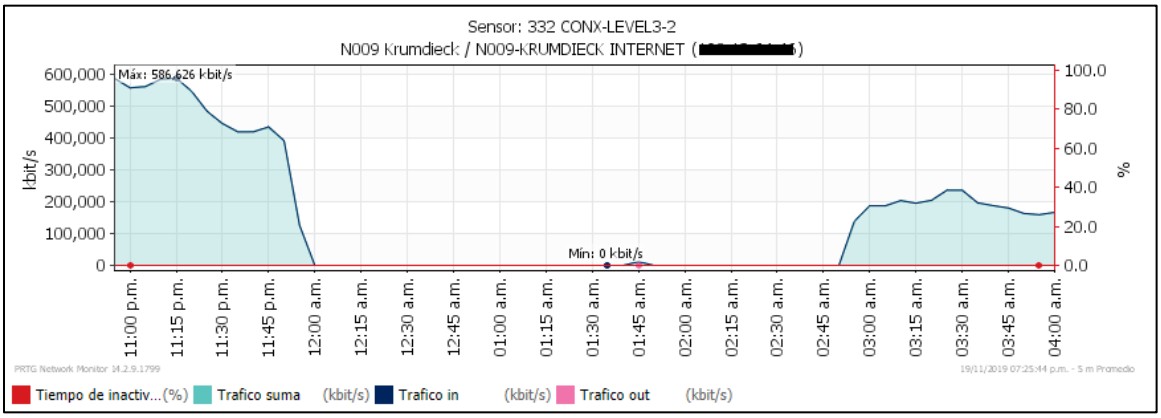


Figura 38 Apagado de interfaz asociado al proveedor CenturyLink

Se visualiza que el tráfico es asumido por el enlace de respaldo del proveedor Telxius.

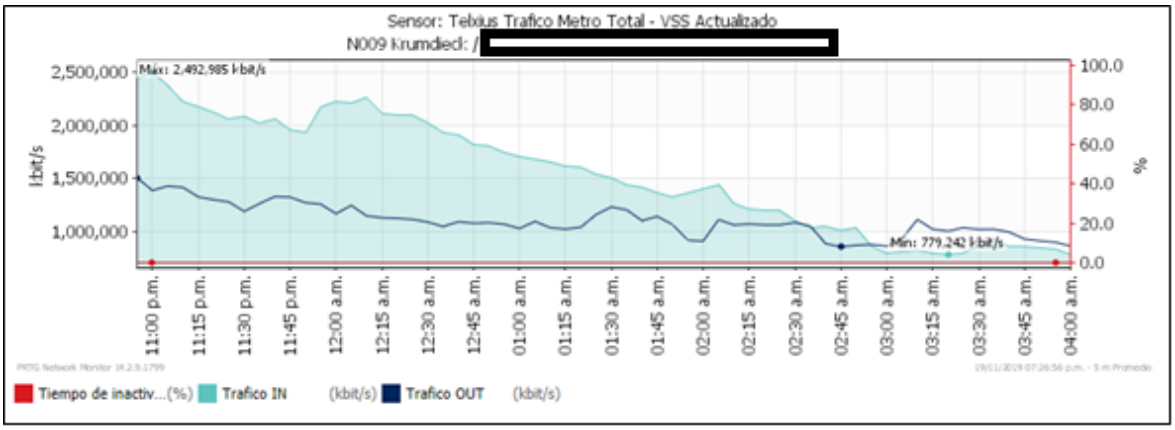


Figura 39 Trafico asumido por interfaz asociado al proveedor Telxius

Actividad 2: Prueba de redundancia de Telxius a Level 3 (CenturyLink).

Se desactiva el tráfico proveniente del proveedor Telxius.

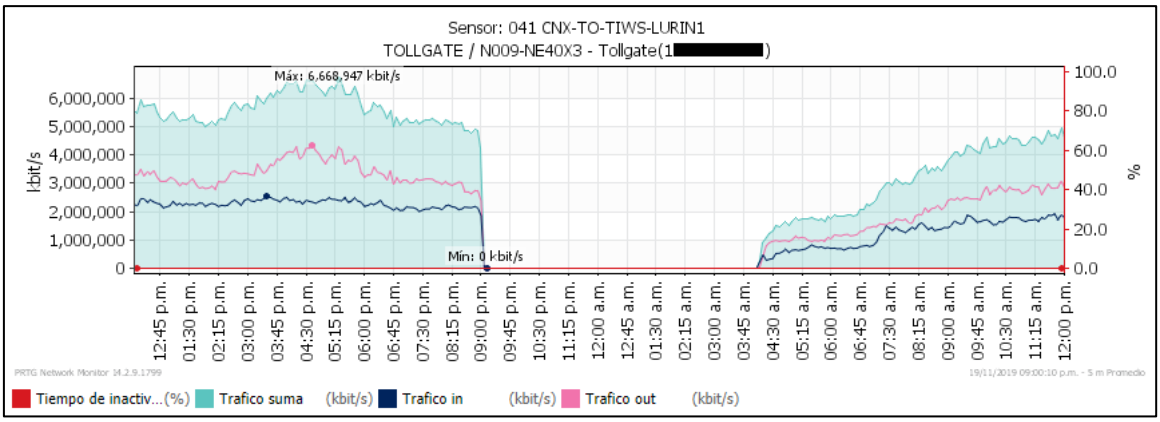


Figura 40 Apagado de interfaz asociado al proveedor Telxius

El tráfico es asumido por el enlace de respaldo del proveedor Level 3 (CenturyLink).

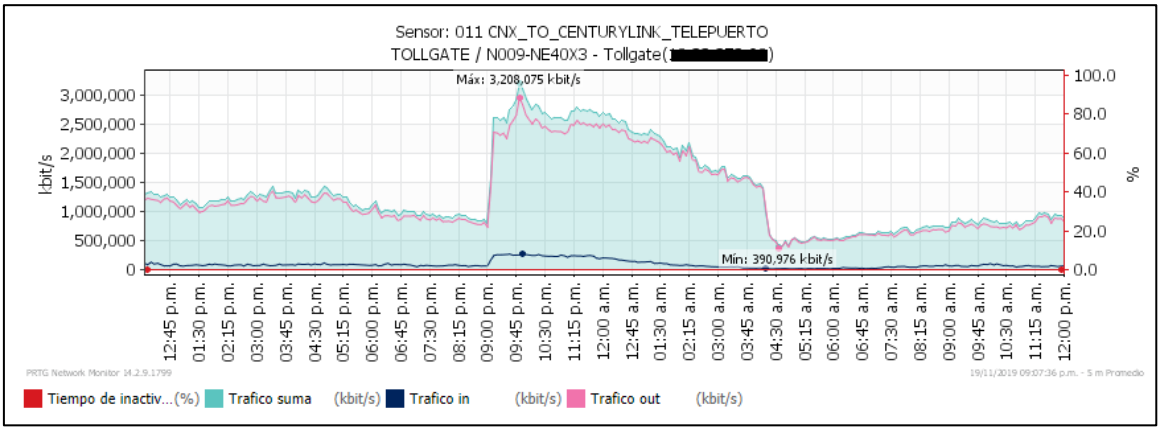


Figura 41 Trafico asumido por la interfaz asociada al proveedor CenturyLink

Conclusiones:

- Con las pruebas realizadas se demostró que las configuraciones realizadas en los equipos de borde son correctas y permiten la conmutación del tráfico de manera automática.
- Las pruebas realizadas demuestran que ambos proveedores están preparados para recibir el tráfico en caso uno de ellos no esté disponible, permitiendo una disponibilidad del servicio.

4.11.4 Ensayo de TAC y NOC alterno.

Escenarios de desastre:

- Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias.

Proceso de negocio afectado:

- Internet
- Interconexión de sedes
- Servicios gestionados

Ensayo 1

Objetivo:

El propósito de esta esta prueba es simular la afectación de las oficinas del área NOC y TAC, y poder reactivar las operaciones de atención de Clientes y monitoreo de la red desde los sitios designados.

Lugar y Fecha:

El ejercicio se realizó en la ciudad de Lima en el distrito de San Borja el día 31 de mayo del año 2019 de hora 10:00 am a 11:00 am. (patio de la sede Gálvez II)

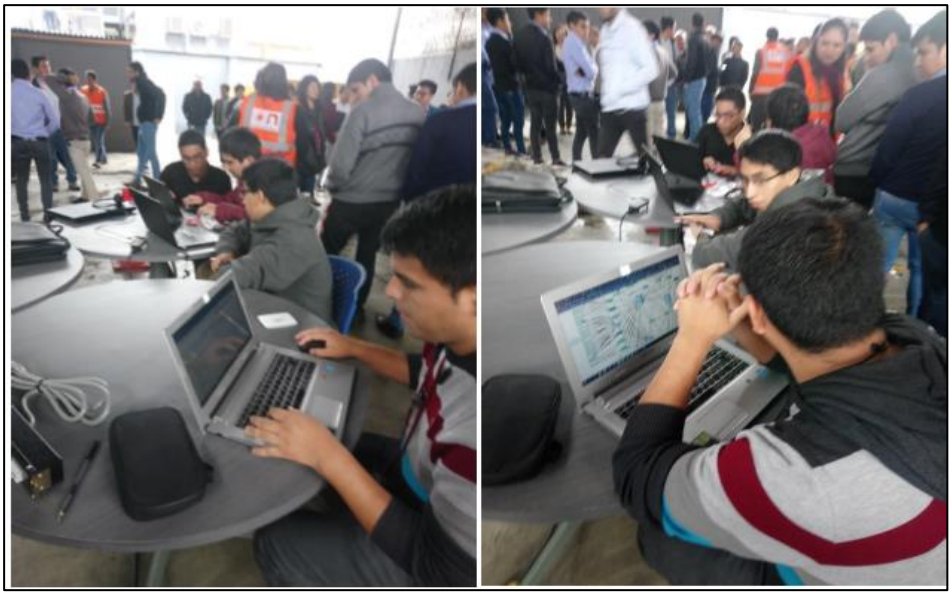


Figura 42 Personal en ensayo de TAC y NOC alterno Sede 1

Conclusiones:

- El sitio de recuperación no era adecuado debido a problemas climatológicos que afectaron el lugar de trabajo.
- Lugar de trabajo se compartía con la zona de evacuación.

- Conexión internet inalámbrico inestable no apto para este tipo de escenario.
- Se recomienda realizar pruebas en un ambiente adecuado para esta tarea.

Ensayo 2

Objetivo:

El propósito de esta esta prueba es simular la afectación de las oficinas del área NOC y TAC, y poder reactivar las operaciones de atención de Clientes y monitoreo de la red desde los sitios designados.

Lugar y Fecha:

El ejercicio se realizó en la ciudad de Lima en el distrito de La Victoria el día 27 de junio del año 2019 de hora 04:00 pm a 5:00 pm. (sede Krumdieck)

Figura 43 Personal en ensayo de TAC y NOC alterno Sede 2

Conclusiones:

- Se encontró el ambiente adecuado para realizar el ejercicio del plan de continuidad.
- La sede de Krumdieck cuenta con acceso a red que brinda el servicio objeto de prueba.
- Se demuestra que en la sede Krumdieck se puede recuperar el servicio de TAC y NOC para la atención a nuestros clientes.

Plan de entrenamiento

Objetivo:

El objetivo del plan de entrenamiento es contar con el personal capacitado en sus respectivas funciones, y que sean capaces de responder de manera efectiva durante un escenario real.

Elementos del plan de entrenamiento:

1. Propósito del DRP: El personal debe conocer el propósito del plan de recuperación ante desastres y sus alcances de manera macro, así mismo entender la importancia de su participación dentro del mismo y el valor que aporta a la compañía.
2. Coordinación y comunicación entre equipos: Es importante que el personal que participa dentro del DRP conozca el árbol de comunicaciones, y la conformación de los equipos, tanto del personal principal como de los suplentes, para que la comunicación fluya de manera correcta según lo planificado.
3. Procedimiento de seguridad: el personal debe estar capacitado en cuanto a medidas de seguridad se refiere para salvaguardar su seguridad personal y la de sus compañeros.
4. Procesos específicos del equipo: El personal debe conocer a detalle los procesos que corresponden al equipo tales como (fases de activación y notificación, recuperación y reconstitución), para ello se debe reforzar con la participación de los equipos en las pruebas y simulacros.
5. Responsabilidades individuales: El personal debe conocer a detalle los procesos individuales tales como (fases de activación y notificación, recuperación y reconstitución), para ello se debe reforzar con la participación del personal en las pruebas y simulacros.

Tabla 46 plan de entrenamiento

Contenido	Participantes	Fechas
Contenido del plan de recuperación	Todos los equipos	Abril
Coordinación entre equipos y árbol de comunicaciones	Todos los equipos	Abril
Plan de seguridad anual	Todo el personal	Mayo

Procesos específicos por equipo de respuesta	Cada equipo de respuesta de manera individual	Mayo

4.12 Plan de mantenimiento

Como parte de la política del plan de recuperación, es necesario mantener actualizado el DRP, debido a que durante la fase de operación existen cambios frecuentes en la organización y es por ello que se debe llevar un control de todos los cambios y ser reportados al área de procesos.

Los cambios en la organización que deben ser considerados a nivel de recursos humanos, implementación de nuevos procesos, adquisición y creación de nuevos productos, requerimiento de seguridad entre otros.

Una parte vital para mantener actualizado el plan, es tener una revisión de todo el plan al menos una vez al año con todos los interesados.

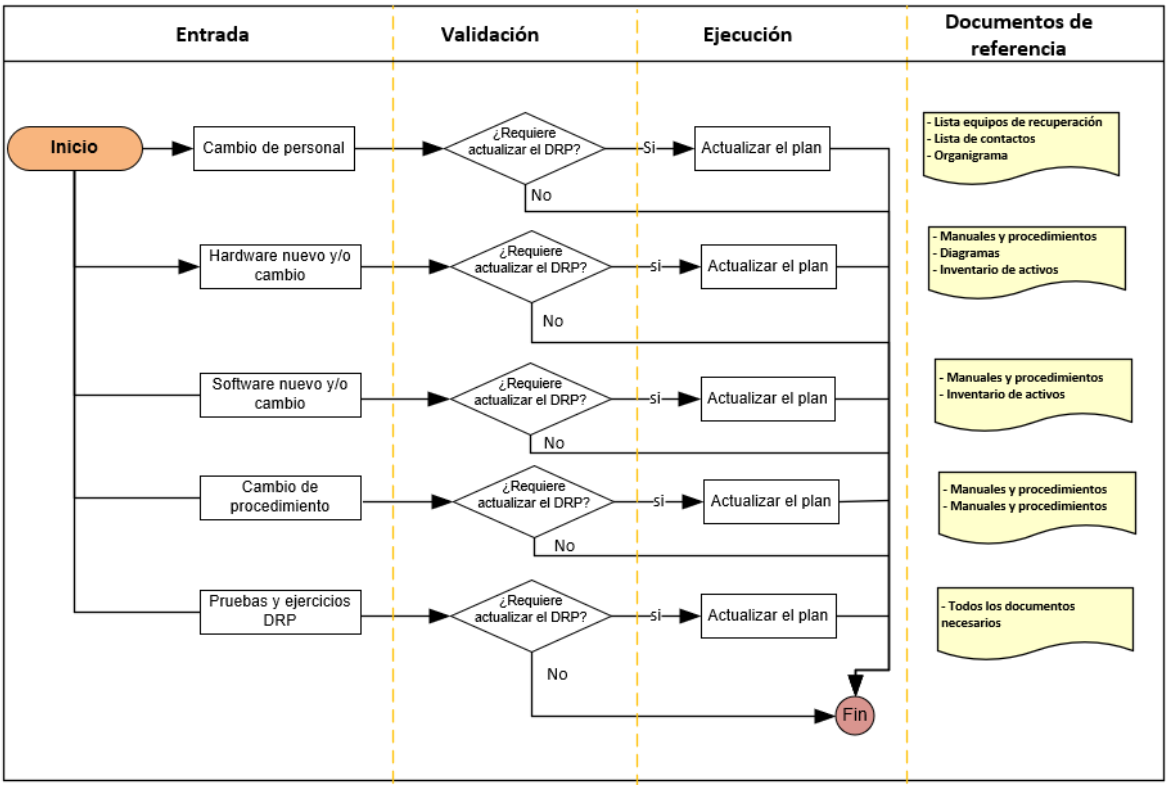


Figura 44 Plan de mantenimiento de DRP
Fuente: Elaboración propia

Registro y control de cambios

Para llevar a cabo cualquier actualización del plan se recomienda realizar un registro de todos los cambios realizados y se lleve un control de los mismos en base a versiones de cada documento con el responsable de cada uno de los cambios realizados.

Tabla 47 Formato de control de cambios

Versión N°	Fecha	Cambios Realizados	Responsable del cambio	Firma

Tabla 48 Cronograma de mantenimiento del DRP

Actividad	Descripción de la actividad	Fecha
Revisión anual del Plan de recuperación.	Esta actividad tiene la finalidad de revisar todo el plan e identificar las oportunidades de mejora en base a las pruebas ejecutadas y realizar los cambios que el core de negocio lo requiera.	23/03/2020 – 28/03/2020
Sismo mayor de 6 hasta 8 grados que afecta la sede principal.	Esta actividad tiene la finalidad de realizar un simulacro de sismo con todo el personal y realizar pruebas de supervivencia de las salas de monitoreo TAC y NOC.	31/05/2020
Incendio que afecta el local del Data Center principal.	Esta actividad tiene la finalidad de simular la afectación del datacenter principal y realizar la prueba de redundancia de los equipos core en el datacenter de respaldo.	28/06/2020
Inundación que afecta el local del Data Center principal.	Esta actividad tiene la finalidad de simular la afectación del datacenter principal y realizar la prueba de redundancia de los equipos core en el datacenter de respaldo.	28/06/2020
Falla de Suministro de Energía Eléctrica mayor a 12 horas que afecta el local del Data Center Principal.	Esta actividad tiene la finalidad de simular la falla de suministro eléctrico y poner a prueba el funcionamiento correcto de los sistemas de UPS y los generadores eléctricos.	28/07/2020
Ataque DDoS mayor a 20GB y/o por más de 10 horas.	Esta actividad tiene la finalidad de probar las herramientas y procedimientos de mitigación contra ataques de tipo DDoS mayores a 10Gbps.	16/08/2020

5 PRUEBAS, RESULTADOS Y VALIDACIÓN

En este capítulo se realizará las pruebas enfocadas en el cumplimiento de cada uno de los objetivos específicos planteados, en base a las métricas e indicadores de logros de objetivos en el capítulo 1.6

A continuación, se hace un resumen los objetivos específicos, sus indicadores de logros y cada uno de sus requerimientos establecidos.

Tabla 49 Resumen de requisitos del objetivo 1

Objetivo específico	Indicador de logro	Métrica	Requerimientos
Identificar los procesos críticos de la compañía que permita calcular el impacto operacional y financiero, para su priorización ante un desastre.	Análisis de impacto de negocio (BIA).	N° de procesos críticos. Cálculo de: RTO RPO MTD	1) Se debe Identificar los procesos críticos de la compañía y evaluar el tipo de impacto. 2) Se debe determinar el impacto financiero estimado por cada uno de los procesos identificados. 3) Se debe calcular los valores para: MTD (tiempo de inactividad máximo tolerable) RTO (Tiempo Objetivo de Recuperación) RPO (Punto Objetivo de Recuperación) 4) Se debe documentar el BIA con todos los requerimientos anteriores.

Tabla 50 Resumen de requisitos del objetivo 2

Objetivo Específico	Indicador de Logro	Métrica	Requerimientos
Identificar los escenarios y los riesgos críticos que puedan impactar el normal funcionamiento de los procesos críticos del negocio.	Matriz de riesgos.	% de riesgos por nivel de criticidad	1) Se debe realizar un inventario de todos los recursos críticos de la compañía y establecer su nivel de criticidad. 2) Se debe identificar los riesgos de los recursos críticos y establecer su probabilidad de ocurrencia y el nivel de impacto sobre los servicios críticos de la compañía. 3) Se debe realizar un tratamiento de los riesgos que se encuentren en la categoría de riesgo intolerable. 4) Se debe identificar los escenarios que puedan afectar a los procesos críticos de negocio y definir sus impactos potenciales.

Tabla 51 Resumen de requisitos del objetivo 3

Objetivo Específico	Indicador de Logro	Métrica	Requerimientos
Desarrollar estrategias y procedimientos de recuperación para los escenarios definidos.	Informe de estrategias y procedimientos.	N° de estrategias por escenario. Eficiencia Costos	1) Se debe identificar los recursos necesarios para cada uno de los escenarios identificados.
			2) Se debe desarrollar una o más estrategias por cada uno de los escenarios identificados.
			3) Se debe desarrollar manuales y procedimientos por cada uno de los escenarios identificados.
			4) Se debe definir los roles y responsabilidades por cada una de las estrategias.

5.1 Plan de pruebas (para el OE1)

5.1.1 Propósitos de la evaluación

Comprobar que los procesos críticos del negocio hayan sido identificados correctamente durante el desarrollo del BIA y del análisis de riesgos, además de que estos cumplan con los objetivos específicos del proyecto y de los requerimientos definidos en el capítulo 3.3.

5.1.2 Alcance de evaluación

a) Validación de los procesos críticos de la compañía,
b) evaluación de los tipos de impacto para los procesos críticos del negocio.
c) Validación de los indicadores: RTO, RPO y MTD

5.1.3 Recursos para las pruebas

a) Recursos TI
   i. Software: Bizagi Modeler
   ii. Equipo de Computo

5.1.4 Estrategia de verificación

Para la evaluación se realizó cuestionarios al personal clave de la compañía para validar los datos.

También se realizará un diagrama de actividades mediante un caso de uso. El cual es necesario para contar con un esquema de flujo de actividades que permitirán determinar el cumplimiento de los requerimientos.

5.1.5 Diagrama de actividades

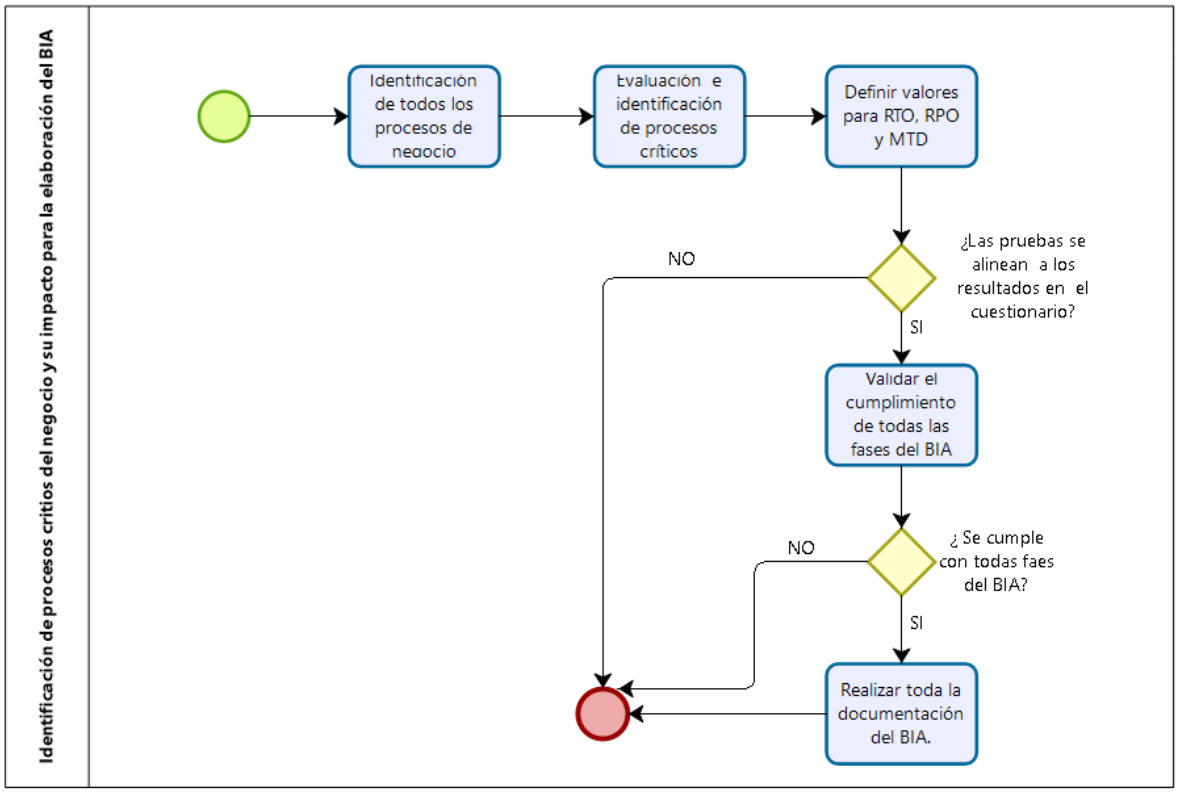


Figura 45 Flujo de actividades para la comprobación del objetivo 1
Fuente: elaboración propia

5.1.6 Casos de prueba de uso

PLAN DE PRUEBAS 1 (PARA OE1)		
Tipo de Prueba: Procesos críticos del negocio y su impacto		
Caso de Prueba: BIA		**Autor del Caso de Prueba:** E.D
Versión del caso de Prueba: 1.0		**Fecha de Creación:** 07/10/2019
Ambiente de Prueba: Cuestionario		**Fecha de Ejecución:** 07/10/2019
Objetivo de Prueba: Evaluar que todas las fases del BIA se encuentren alineadas a las necesidades del negocio.		**Criterios de éxito y fracaso:** **Éxito:** Todas las fases del BIA están alineados al negocio. **Fracaso:** las fases del BIA NO están alineadas al negocio.
Flujo de pasos de la Prueba		
Nro	**Descripción del Paso**	**Resultado Esperado**
1	Identificación de los procesos del negocio.	Se realiza el listado de todos los procesos del negocio. Se identifican 9 procesos de negocio: 1) Internet 2) Interconexión de sedes (L2L)

<table>
<tr><td></td><td></td><td>3) Servicios gestionados (S.G)
4) Telefonía
5) Servicios en la nube
6) Servicios adicionales
7) Centro de datos
8) Lan center
9) Streaming</td></tr>
<tr><td>2</td><td>Evaluación e identificación de los procesos críticos del negocio, en base al impacto financiero.</td><td>Se realizó la evaluación de 9 procesos de negocio, de los cuales se identificó 3 procesos críticos en base al impacto financiero (% de facturación anual)
<table>
<tr><th>Procesos críticos identificados</th><th>Impacto Financiero</th><th>% de facturación anual.</th><th>Estimación de pérdidas económicas por hora</th></tr>
<tr><td>Internet</td><td>Alto</td><td>45%</td><td>S/ 199 325.39</td></tr>
<tr><td>Interconexión de sedes (L2L)</td><td>Alto</td><td>30%</td><td>S/ 153 374.72</td></tr>
<tr><td>Servicios Gestionados</td><td>Medio</td><td>15%</td><td>S/ 12 801.01</td></tr>
</table></td></tr>
<tr><td>3</td><td>Identificación de valores para:
MTD (tiempo de inactividad máximo tolerable)
RTO (Tiempo Objetivo de Recuperación)
WRT (Tiempo de trabajo en Recuperación)
RPO (Punto Objetivo de Recuperación)</td><td>Para determinar los valores descritos en la tabla se tomó en consideración 9 factores en base experiencias pasadas y lecciones aprendidas, y entrevistas realizadas al gerente de redes.
<table>
<tr><th>Procesos críticos</th><th>RPO</th><th>RTO</th><th>WRT</th><th>MTD</th></tr>
<tr><td>Internet</td><td>2 horas</td><td>2 horas</td><td>1 horas</td><td>2 horas</td></tr>
<tr><td>Interconexión de sedes (L2L)</td><td>2 horas</td><td>3 horas</td><td>2 horas</td><td>5 horas</td></tr>
<tr><td>Servicios gestionados</td><td>2 horas</td><td>3 horas</td><td>2 horas</td><td>5 horas</td></tr>
</table></td></tr>
<tr><td rowspan="2">4</td><td rowspan="2">¿Las pruebas realizadas y los resultados obtenidos se encuentran alineadas con los resultados obtenidos en el cuestionario realizado al personal clave de la compañía?</td><td>SI: En base a la evaluación realizada se determina que los datos obtenidos se encuentran alineados a los resultados obtenidos en el cuestionario. (X)
Revistar el anexo (y)</td></tr>
<tr><td>No: En base a la evaluación realizada se determina que los datos obtenidos no se encuentran alineados a los resultados obtenidos en el cuestionario</td></tr>
</table>

<table>
<tr><td>5</td><td>Realizar la validación del cumplimiento de todos los componentes y actividades que comprenden el BIA.</td><td>Se realiza un listado de actividades y su estado:
<table><tr><th>Componentes del BIA</th><th>Estado</th></tr><tr><td>Identificación de procesos críticos del negocio</td><td>Realizado</td></tr><tr><td>Medición del impacto de los Procesos críticos</td><td>Realizado</td></tr><tr><td>Medición del impacto financiero</td><td>Realizado</td></tr><tr><td>Determinación del MTD, RTO y RPO</td><td>Realizado</td></tr><tr><td>Identificación de activos que soportan el negocio</td><td>Realizado</td></tr></table></td></tr>
<tr><td rowspan="2">6</td><td rowspan="2">¿Se cumplió con todas las fases del BIA?</td><td>SI: En base a la validación de todos los componentes se determina el cumplimiento de todas las fases del BIA. (X)</td></tr>
<tr><td>NO: En base a la validación de todos los componentes se determina el cumplimiento de todas las fases del BIA.</td></tr>
<tr><td>7</td><td>Realizar la documentación completa del BIA</td><td>La documentación completa del BIA se realizó en el capítulo 4.2</td></tr>
<tr><td colspan="3">Decisión de aprobación del caso de prueba: Aprobó_X_ Fallo____</td></tr>
<tr><td colspan="2">Fecha de aprobación del caso de prueba</td><td>10/10/2019</td></tr>
</table>

5.1.7 Objetivos del indicador

Porcentaje de procesos críticos del negocio identificados

Calculo:

$$\frac{\text{Cantidad de procesos criticos identificados (3)}}{\text{Cantidad Total procesos de negocio identificados (10)}} * 100 = 33\%$$

De acuerdo con lo realizado durante el proceso de elaboración del BIA, se identificó 3 procesos críticos del negocio lo cuales representan un 33% de todas las operaciones que se deben tener en cuenta para el desarrollo de las estrategias de elaboración del DRP

5.2 Plan de pruebas (para el OE2)

5.2.1 Propósitos de la evaluación

Comprobar que se hayan identificado correctamente los escenarios y riesgos que puedan impactar en los procesos de negocio, así como el cumplimiento de todos los requisitos establecidos para este objetivo específico.

5.2.2 Alcance de la evaluación

a) Validación del inventario de recursos críticos de la compañía.
b) Validar de la realización del análisis de riesgo.
c) Validación de la realización del tratamiento de los riesgos.
d) Validación de los escenarios de desastre identificados.

5.2.3 Recursos para las pruebas

a) Recursos TI
   i. Software: Bizagi Modeler
   ii. Equipo de Computo

5.2.4 Estrategia de verificación

Para la evaluación se realizó cuestionarios al personal clave de la compañía para validar los datos.

También se realizará un diagrama de actividades mediante un caso de uso. El cual es necesario para contar con un esquema de flujo de actividades que permitirán determinar el cumplimiento de los requerimientos.

5.2.5 Diagrama de actividades

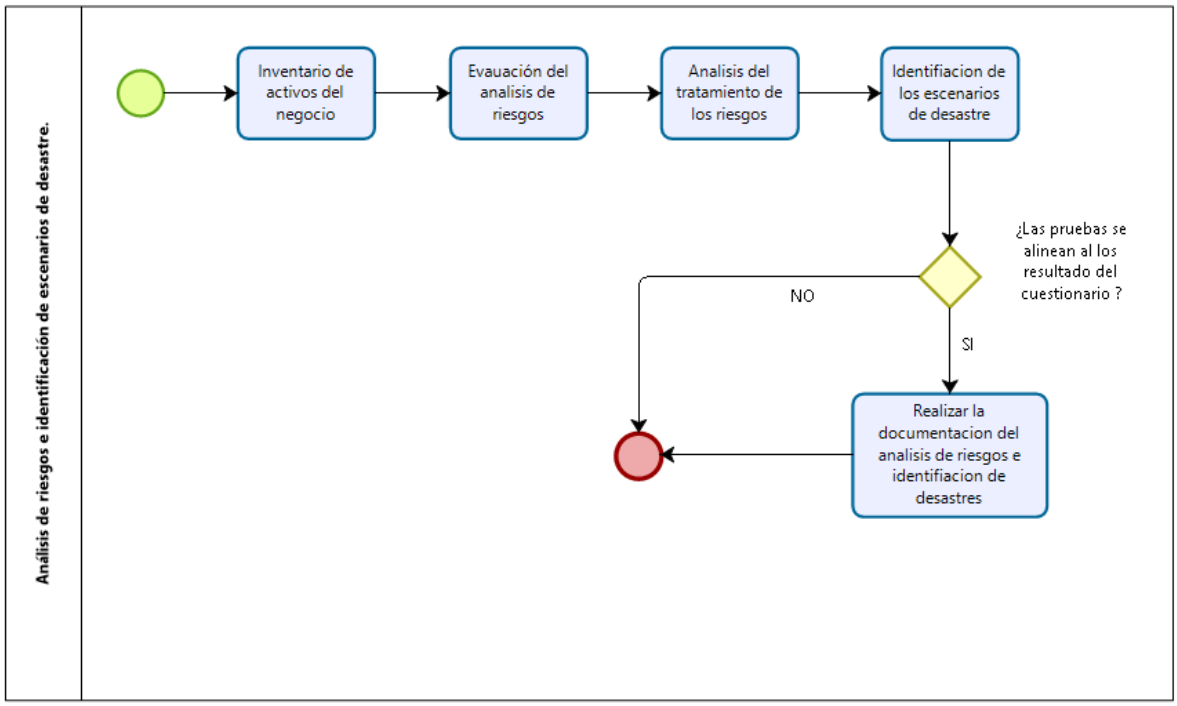


Figura 46 Flujo de actividades para la comprobación del objetivo 2
Fuente: elaboración propia

5.2.6 Casos de prueba de uso

<table>
<tr><td colspan="3">PLAN DE PRUEBAS 1 (PARA OE2)</td></tr>
<tr><td colspan="3">Tipo de Prueba: Proceso de análisis de riesgos críticos y escenarios de desastre</td></tr>
<tr><td colspan="2">Caso de Prueba: Análisis de riesgos</td><td>Autor del Caso de Prueba: E.D</td></tr>
<tr><td colspan="2">Versión del caso de Prueba: 1.0</td><td>Fecha de Creación: 07/10/2019</td></tr>
<tr><td colspan="2">Ambiente de Prueba: Cuestionario</td><td>Fecha de Ejecución: 07/10/2019</td></tr>
<tr><td colspan="2">Objetivo de Prueba: Evaluar el desarrollo del análisis de riesgos y escenarios de desastre.</td><td>Criterios de éxito y fracaso:
Éxito: El análisis de riesgo y los escenarios están alineados al negocio.
Fracaso: El análisis de riesgo y los escenarios NO están alineados al negocio.</td></tr>
<tr><td colspan="3">Flujo de pasos de la Prueba</td></tr>
<tr><td>Nro</td><td>Descripción del Paso</td><td>Resultado Esperado</td></tr>
<tr><td>1</td><td>Identificación de recursos críticos del negocio.</td><td>Para esta actividad se realizó un inventario de los recursos que soportan los procesos críticos del negocio y se determinó su nivel de criticidad.
<table>
<tr><th>Criticidad</th><th>Cantidad de recursos</th></tr>
<tr><td>Alta</td><td>20</td></tr>
<tr><td>Media</td><td>20</td></tr>
<tr><td>Baja</td><td>3</td></tr>
</table></td></tr>
<tr><td>2</td><td>Evaluación de análisis de riesgos</td><td>En esta actividad se realizó el análisis de riesgos de todos los recursos con cada una de las amenazas identificadas.
<table>
<tr><th>Cantidad de amenazas por recurso</th><th colspan="2">Probabilidad de ocurrencia</th><th colspan="2">Impacto</th><th colspan="2">Nivel de riesgo</th><th colspan="2">Nivel de Tolerancia</th></tr>
<tr><td rowspan="4">63</td><td>Muy Baja</td><td>2</td><td>Muy Baja</td><td>0</td><td>Muy Baja</td><td>0</td><td>Tolerable</td><td>10</td></tr>
<tr><td>Baja</td><td>45</td><td>Baja</td><td>13</td><td>Baja</td><td>10</td><td>Moderado</td><td>41</td></tr>
<tr><td>Media</td><td>13</td><td>Media</td><td>39</td><td>Media</td><td>41</td><td rowspan="2">Intolerable</td><td rowspan="2">12</td></tr>
<tr><td>Alta</td><td>3</td><td>Alta</td><td>11</td><td>Alta</td><td>12</td></tr>
</table></td></tr>
<tr><td>3</td><td>Análisis de los Tratamiento de los riesgos</td><td>En este análisis se identificó 12 riesgos intolerables de los cuales se le hizo un tratamiento mediante estrategias.
<table>
<tr><th>Riesgos Intolerables</th><th colspan="2">Estrategia</th></tr>
<tr><td rowspan="3">12</td><td>Transferir</td><td>4</td></tr>
<tr><td>Mitigar (reducir)</td><td>8</td></tr>
<tr><td>Aceptar</td><td>0</td></tr>
</table></td></tr>
</table>

4	Evaluación del escenario de desastre identificados.	En esta actividad se identificó 6 escenarios críticos para los procesos de negocio, los cuales fueron analizados para la elaboración de las estrategias del DRP. • Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias • Ataque DDoS mayor a 20Gbps y/o por más de 10 horas. • Incendio que afecta local del Data Center principal (DC1). • Inundación que afecta el Local del Data Center Principal (DC1). • Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1). • Ausencia de personal especializado por fallecimiento o enfermedad.
5	¿Las pruebas realizadas y los resultados obtenidos se encuentran alineadas con los resultados obtenidos en el cuestionario realizado al personal clave de la compañía?	SI: En base a la evaluación realizada se determina que los datos obtenidos se encuentran alineados a los resultados obtenidos en el cuestionario. **(X)** Revistar el anexo (y)
		No: En base a la evaluación realizada se determina que los datos obtenidos no se encuentran alineados a los resultados obtenidos en el cuestionario
6	Realizar la documentación completa del análisis de riesgos	La documentación completa del BIA se realizó en el capítulo 4.3 y 4.5
Decisión de aprobación del caso de prueba: Aprobó_X_ Fallo____		
Fecha de aprobación del caso de prueba		10/10/2019

5.2.7 Objetivos del indicador

Porcentaje de amenazas identificadas con riesgo tolerables

Calculo:

$$\frac{\text{Cantidad de Riesgos tolerables (10)}}{\text{Cantidad Total de riesgos identificadas (63)}} * 100 = 16\%$$

Se identificó un 16% de los riesgos que son tolerables que no requieren un tratamiento especial y que no representan amenazas que puedan impactar en los procesos críticos del negocio.

Porcentaje de amenazas identificadas con riesgo moderado

Calculo:

$$\frac{\text{Cantidad de Riesgos moderado (41)}}{\text{Cantidad Total de riesgos identificadas (63)}} * 100 = 65\%$$

Se identificó un 65% de los riesgos que son moderados y pueden ser mitigados con estrategias de contingencias a fin de no generar un impacto alto en los procesos de negocio.

Porcentaje de amenazas identificadas con riesgo intolerable

Calculo:

$$\frac{\text{Cantidad de Riesgos Intolerables (12)}}{\text{Cantidad Total de riesgos identificadas (63)}} * 100 = 19\%$$

Se identificó un 19% de los riesgos que han sido clasificado como riesgos intolerables, para lo cual se debe establecer estrategias de contingencias.

5.3 Plan de pruebas (para el OE3)

5.3.1 Propósitos de la evaluación

Comprobar que las estrategias de recuperación definidas cumplan con todos los requerimientos establecidos, así mismo que estén alineados a los procesos de negocio críticos.

5.3.2 Alcance de la evaluación

a) Validación de todos los recursos necesarios para cada escenario.
b) Validación de todas estrategias desarrolladas para cada escenario.
c) Validación del desarrollo de manuales y procedimiento para los escenarios.
d) Validación de los roles y responsabilidades

5.3.3 Recursos para las pruebas

a) Recursos TI

iii. Software: Bizagi Modeler

iv. Equipo de Computo

5.3.4 Estrategia de verificación

Se realizará un diagrama de actividades mediante un caso de uso. El cual es necesario para contar con un esquema de flujo de actividades que permitirán determinar el cumplimiento de los requerimientos.

5.3.5 Diagrama de actividades

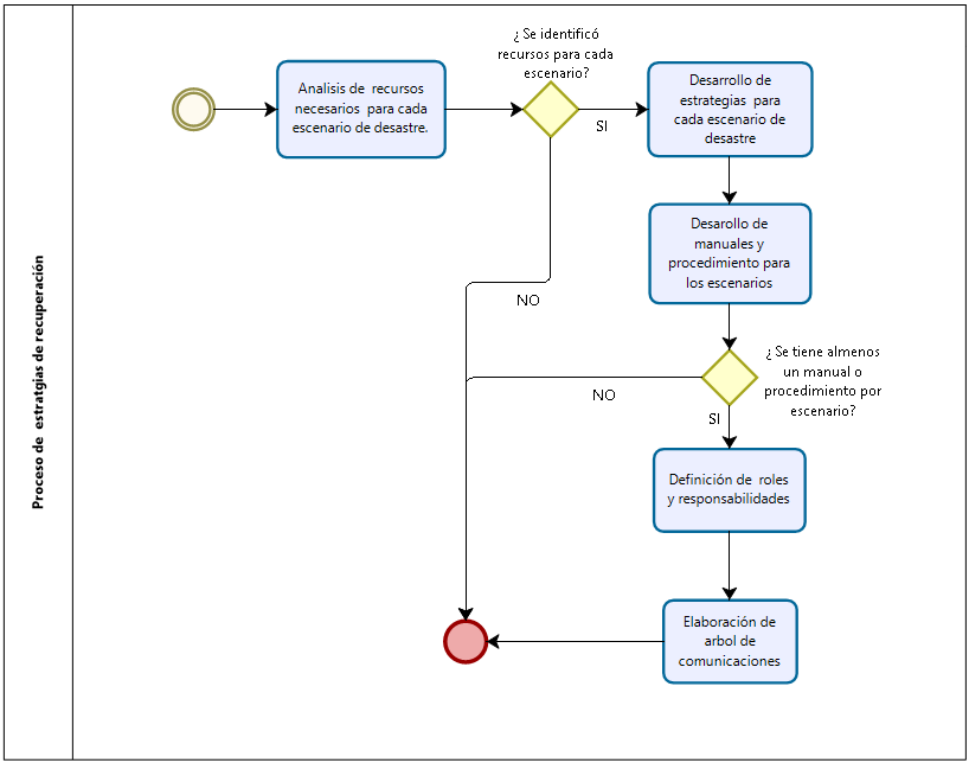


Figura 47 Flujo de actividades para la comprobación del objetivo 3

Fuente: elaboración propia

5.3.6 Casos de prueba de uso

PLAN DE PRUEBAS 1 (PARA OE3)	
Tipo de Prueba: Estrategias de recuperación	
Caso de Prueba: Estrategias y procedimientos de recuperación.	**Autor del Caso de Prueba:** E.D
Versión del caso de Prueba: 1.0	**Fecha de Creación:** 07/10/2019

<table>
<tr><td colspan="2">Ambiente de Prueba: Cuestionario</td><td>Fecha de Ejecución: 07/10/2019</td></tr>
<tr><td colspan="2">Objetivo de Prueba: Evaluar el desarrollo de las estrategias de recuperación, así como los manuales y procedimientos</td><td>Criterios de éxito y fracaso:
Éxito: Las estrategias de recuperación y los procedimientos están alineados al negocio.
Fracaso: Las estrategias de recuperación y los procedimientos NO están alineados al negocio.</td></tr>
<tr><td colspan="3">Flujo de pasos de la Prueba</td></tr>
<tr><td>Nro</td><td>Descripción del Paso</td><td>Resultado Esperado</td></tr>
<tr><td>1</td><td>Identificación de recursos necesarios para cada escenario.</td><td>Para esta actividad Se realizó la identificación de los recursos necesarios para cada uno de los escenarios definidos.
Personas.
Información y datos.
Edificios, entorno de trabajo y servicios asociados.
instalaciones, equipos y consumibles.
Sistemas de tecnología de la información y la comunicación.
Transportes.</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">¿Se identificó los recursos para cada escenario?</td><td>SI: Se identificaron todos los recursos necesarios para cada uno de los escenarios de desastre identificados. (X)</td></tr>
<tr><td>NO: no Se identificaron todos los recursos necesarios para cada uno de los escenarios de desastre identificados.</td></tr>
<tr><td>3</td><td>Estrategias para cada escenario de desastre.</td><td>En esta actividad se desarrolló estrategias para cada escenario de desastre
<table><tr><th>Escenarios de desastre</th><th>Código de estrategia</th></tr><tr><td>Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias</td><td>E001</td></tr><tr><td>Ataque DDoS mayor a 20Gbps y/o por más de 10 horas.</td><td>E002, E002.1</td></tr><tr><td>Incendio que afecta local del Data Center principal (DC1).</td><td>E003</td></tr><tr><td>Inundación que afecta el Local del Data Center Principal (DC1).</td><td>E004</td></tr><tr><td>Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1).</td><td>E005</td></tr><tr><td>Ausencia de personal especializado por fallecimiento o enfermedad.</td><td>E006</td></tr></table></td></tr>
<tr><td>4</td><td>Desarrollo de manuales y procedimientos para cada escenario de desastre identificado.</td><td>En esta actividad Se desarrolló manuales y procedimientos para cada una de las estrategias definidas</td></tr>
</table>

<table>
<tr><td></td><td></td><td><table>
<tr><th>Código de estrategia</th><th>Manuales y procedimientos.</th></tr>
<tr><td>E001</td><td>Manual recuperación de backbone DC2</td></tr>
<tr><td>E002</td><td>Manual mitigación de herramienta Arbor</td></tr>
<tr><td>E002.1</td><td>Manual de mitigación con blackhole</td></tr>
<tr><td>E003</td><td>Manual recuperación de backbone DC2</td></tr>
<tr><td>E004</td><td>Manual recuperación de backbone DC2</td></tr>
<tr><td>E005</td><td>Manual recuperación de backbone DC2</td></tr>
<tr><td>E006</td><td>Procedimiento de activación de protocolo de personal especializado externo.</td></tr>
</table></td></tr>
<tr><td rowspan="2">5</td><td rowspan="2">¿Se desarrolló al menos un manual o procedimiento por cada uno de los escenarios y estrategias de recuperación?</td><td>SI: Se desarrolló procedimientos por cada una de las estrategias de recuperaciones definidas. (X)</td></tr>
<tr><td>No: no Se desarrolló procedimientos por cada una de las estrategias de recuperaciones</td></tr>
<tr><td>6</td><td>Definición de roles y responsabilidades.</td><td>Se realizó la definición de los roles y responsabilidades para las estrategias de recuperación, el cual se detalla en el capítulo 4.9</td></tr>
<tr><td>7</td><td>Elaboración de árbol de comunicaciones.</td><td>Se definió un árbol de comunicaciones del personal clave de la organización en el capítulo 4.10</td></tr>
<tr><td colspan="3">Decisión de aprobación del caso de prueba: Aprobó_X_ Fallo____</td></tr>
<tr><td colspan="2">Fecha de aprobación del caso de prueba</td><td>10/10/2019</td></tr>
</table>

5.4 Análisis de resultados de pruebas TT&E

5.4.1 Análisis de resultados de prueba 1

Como parte de las pruebas se realizó la simulación de la falla de equipos de Core del datacenter principal, para lo cual se consideró los escenarios de desastre y los procesos críticos que se afectarían en un escenario real.

Tabla 52 Relación entre prueba 1, escenarios y procesos críticos.

Prueba	Escenario de desastre	Procesos críticos afectados
Simulación de falla de equipos Core-INT	Incendio que afecta local del Data Center principal (DC1).	• Internet
	Inundación que afecta el Local del Data Center Principal (DC1).	
	Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1).	
	Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias.	
Simulación de falla de equipos Core-AGG	Incendio que afecta local del Data Center principal (DC1).	• Internet • Interconexión de sedes • Servicios gestionados
	Inundación que afecta el Local del Data Center Principal (DC1).	
	Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1).	
	Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias.	

Tabla 53 Evaluación de resultados prueba 1

Puntos de evaluación	Medición	Respuesta
Tiempo de coordinación de los integrantes	45 minutos	Regular
Traslado del equipo de respuesta hasta los datacenter.	15 minutos	Bueno
Preparación y coordinación de los equipos de respuesta en los datacenter.	15 minutos	Regular
Conmutación de roles Router de Internet.	10 segundos	Bueno
Apagado de tarjetas del Router de Internet.	3 segundos	Muy bueno
Conmutación de proveedores de internet.	5 segundos	Muy bueno
Conmutación de roles Switch de agregación.	15 segundos	Bueno
Apagado de tarjetas del Switch de agregación.	3 segundos	Muy bueno
Conocimiento del procedimiento de recuperación por parte del equipo de respuesta.	-	Bueno

Observaciones y puntos de mejora

- El equipo de respuesta tardó mucho tiempo en reunirse debido a que no llegaron a la hora pactada.
- Una vez llegado al datacenter principal la comunicación fue defectuosa ya que había poca señal para los teléfonos móviles, se sugiere instalar un teléfono fijo.
- En el datacenter se encontró conexiones sin rotular lo que tomó más tiempo en identificar ciertas conexiones, se sugiere etiquetar todas las conexiones.
- En el datacenter no se contaba con mobiliarios necesarios para que el personal pueda trabajar en condiciones adecuadas.

5.4.2 Análisis de resultados de prueba 2

Tabla 54 Relación entre prueba 2, escenario y procesos críticos.

Prueba	Escenario de desastre	Procesos críticos afectados
Ataque de tipo DDoS superior a los 20 Gbps.	Ataque DDoS mayor a 20Gbps y/o por más de 10 horas.	Internet

Para esta prueba de ataque de tipo DDoS se realizó sobre un entorno real, en donde se validó el cumplimiento del procedimiento y la efectividad de la misma, para ello se tomó los siguientes puntos para su medición:

Tabla 55 Evaluación de resultados prueba 2

Puntos de evaluación	Medición	Repuesta
Detección del ataque	60 segundos	Bueno
Identificación del destino atacado	30 segundos	Bueno
Mitigación con la herramienta local	30 segundos	Bueno
Comunicación con el proveedor Cloud	5 minutos	Regular
Mitigación en la herramienta Cloud	2 minutos	Regular
Pruebas de navegación	2 minutos	Bueno
Comunicación a las otras áreas.	5 minutos	Bueno
Conocimiento del procedimiento de recuperación por parte del equipo de respuesta.	-	Bueno

Observaciones y puntos de mejora

- El equipo de respuesta presentó dificultades en la comunicación con el proveedor Arbor Cloud, debido a que el proveedor solo hablaba inglés, se sugiere reforzar al personal en dicho idioma.
- Durante la detección y mitigación se detectó saturación de los canales, por lo que la sincronización con el proveedor Arbor Cloud tardó 2 minutos, cuando lo planteado es 30 segundos, se sugiere un canal de internet exclusivo para esta señalización.
- Para la mitigación en con la herramienta Cloud requiere una confirmación para iniciar la mitigación, por lo que se sugiere solicitar la mitigación automática sin requerir confirmación.

5.4.3 Análisis de resultados de prueba 3

Tabla 56 Relación entre prueba 3, escenario y procesos críticos**.**

Prueba	Escenario de desastre	Procesos críticos afectados
Prueba de redundancia de enlaces internacionales	Incendio que afecta local del Data Center principal (DC1).	Internet
	Inundación que afecta el Local del Data Center Principal (DC1).	
	Pérdida de Suministro de Energía Eléctrica mayor a 6 horas que afecta el Data center principal (DC1).	
	Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias.	

La prueba de redundancia de enlaces internacionales se realizó un entorno controlado, sobre equipos en producción, para lo cual se tomaron mediciones sobre los siguientes puntos:

Tabla 57 Evaluación de resultados prueba 3

Puntos de evaluación	Medición	Repuesta
Validación previa de todos los prefijos de direcciones IP publica (Actividad previa)	20 minutos	Regular
Desactivar tráfico del proveedor principal	30 segundos	Bueno
Cambio de tráfico por el proveedor secundario	5 segundos	Bueno
Validación del tráfico con las herramientas de monitoreo	2 minutos	Bueno
Capacidad de los enlaces de respaldo para soportar todo el tráfico.	40 Gbps	Bueno
Validación con routers externos	30 segundos	Bueno
Conocimiento del procedimiento del personal	-	Bueno

Observaciones y puntos de mejora

- El procedimiento de validación previo toma mucho tiempo debido a que se trabaja desde un archivo donde se encuentran todos los prefijos en un formato de inventario, se sugiere tener un script con todos los prefijos precargados y se requiera menos trabajo manual.
- La validación de los prefijos luego de la conmutación del tráfico hacia el proveedor secundario se realiza de manera manual, por lo que se sugiere automatizar el proceso.

5.4.4 Análisis de resultados de prueba 4

Tabla 58 Relación entre prueba 3, escenario y procesos críticos.

Prueba	Escenario de desastre	Procesos críticos afectados
Simulación de fallas de salas de monitoreo de TAC y NOC	Sismo mayor a 6 hasta 8 grados que afecta el local principal y sedes secundarias.	• Internet • Interconexión de sedes • Servicios gestionados

El ensayo realizado corresponde a la simulación de la falla de las salas de monitoreo TAC y NOC, por lo que se evaluó el funcionamiento de los sitios alternos:

Tabla 59 Evaluación de resultados prueba 4

Puntos de evaluación	Medición	Repuesta
Acondicionamiento del ambiente para las pruebas	1 hora	Bueno
Traslado del personal a sede de respaldo	20 minutos	bueno
El personal se instala en el ambiente asignado	5 minutos	Bueno
El personal habilita sus herramientas de trabajo	5 minutos	Bueno
Personal recibe llamadas de clientes	7 minutos	Regular
Personal realiza pruebas de todas las herramientas.	1 hora	Regular

Observaciones y puntos de mejora

- Para la primera prueba realizada se encontró un ambiente húmedo y se compartía el espacio con el ambiente de evacuación. (en la segunda prueba se corrigió dicho inconveniente).

- Durante las pruebas se atendió llamadas de clientes, sin embargo, se vio que en un escenario real sería necesario contar con una sala de mayor capacidad en la que puedan trabajar al menos 10 personas, se recomienda establecer un ambiente exclusivo para esta sala de respaldo.

6 CONCLUSIONES

Después de haber desarrollado este proyecto de tesis se presentan las siguientes conclusiones:

1. Se realizó un análisis de impacto de negocio, con lo que se logró definir los procesos críticos del negocio, para ello se analizó factores financieros, reputación, legales y regulatorios, haciendo uso de reuniones y entrevistas al personal de la compañía, con ello se logró determinar que existen 3 procesos fundamentales para la empresa que representan el 90% de sus ingresos anuales.
2. Se desarrolló un análisis de riesgos de los recursos de la compañía asociados a los procesos críticos definidos en el BIA, luego un exhaustivo análisis se identificó que un 19% de los riesgos se encuentran en la categoría intolerable, lo cual fue tomado entrada para la identificación de los escenarios de desastre y sus estrategias de recuperación.
3. Con los análisis previamente realizados se lograron identificar 6 escenarios de desastre que podrían afectar gravemente a la compañía, para lo cual se desarrollaron las estrategias de recuperación, así mismo se analizó los recursos necesarios para cada estrategia.
4. Como parte de las actividades que solicita la norma NIST 800-34, se realizó de manera exitosa pruebas denominadas TT&E, en el que se simuló fallas de los equipos de Core en el datacenter principal, falla de enlaces de proveedores internacionales, ataques de tipo DDoS y así mismo se realizó ejercicios de sitio alterno de monitoreo y atención de clientes para las áreas NOC y TAC, para cada una de estas pruebas se realizó un análisis de los resultados en el capítulo 5.4
5. Se logró cumplir con los objetivos planteados al inicio del proyecto, en el que se no solo se realizó un análisis de escritorio, sino que también se probaron la efectividad de los sistemas de contingencia y los procedimientos de recuperación.

7 RECOMENDACIONES

Para mejorar la efectividad del DRP, garantizar su éxito y continuidad en el futuro se presentan las siguientes recomendaciones:

1. Uno de los activos más importantes de toda organización son las personas, por lo que se debe transmitir a las personas una cultura enfocada en temas de DRP y continuidad de negocios, para lo cual se debe comunicar efectivamente las políticas y concientizar al personal de importancia que este tema merece, por otro lado, hacerlas participe de las actividades que se desarrollen en estos temas.
2. La alta gerencia debe brindar todo el apoyo necesario para el mantenimiento del DRP y debe establecer un presupuesto anual, así mismo hacer parte de sus objetivos estratégicos del año.
3. La tecnología y la infraestructura tanto del hardware como del software que se implemente debe estar enfocado en garantizar un esquema de alta disponibilidad y/o permitir una efectiva recuperación en caso fallaran estos sistemas.
4. Documentar y mantener actualizado el DRP con los cambios realizados a nivel tecnológico y organizacionales, también tomar en cuenta las lecciones aprendidas de los ejercicios realizado para impulsar mejoras en el documento.
5. Capacitar al personal en sus roles y responsabilidades definidas al menos una vez al año, ya que el objetivo es que el personal pueda ejecutar las tareas que le corresponden de manera efectiva en un escenario real.
6. Se debe cumplir con los cronogramas de las pruebas de manera anual, ya que es la única manera de comprobar la efectividad de los sistemas puestos en producción, todas estas pruebas se deben ser documentadas adecuadamente para extraer las oportunidades de mejora. Es fundamental que estas pruebas se realicen sobre ambientes controlados y no generen un impacto en el servicio ofrecido al cliente.

8 REFERENCIAS

Halabi. S.(2003). Metro Ethernet. Estados Unidos: Cisco Press.

Rosen E., & Viswanathan. A (2001). Multiprotocol Label Switching Architecture. Recuperado de https://tools.ietf.org/html/rfc3031 [Consulta: 10 de agosto de 2019].

Kaspersky. (2017). ¿Qué son los ataques DDoS?. Recuperado de https://latam.kaspersky.com/resource-center/threats/ddos-attacks [Consulta: 10 de agosto de 2019].

PCWorld. (2016). Attackers are now abusing exposed LDAP servers to amplify DDoS attacks. Recuperado de https://www.pcworld.com/article/3135771/attackers-are-now-abusing-exposed-ldap-servers-to-amplify-ddos-attacks.html [Consulta: 10 de agosto de 2019].

Deiotte. (2017). Ataque masivo de Ransomware. Recuperado de https://www2.deloitte.com/content/dam/Deloitte/ec/Documents/deloitte-analytics/Estudios/Informe-detallado-Ataque%20masivo-Ransomware-WannaCry-finales.pdf [Consulta: 26 de agosto de 2019].

NAP Perú (2006). Reseña Histórica del NAP Perú. Recuperado de http://www.nap.pe/acerca-del-nap-peru/historia/ [Consulta: 29 de agosto de 2019].

Hervias, V. (2010). Gestionando la Continuidad de nuestro negocio. *AEC: Asociación Española Para La Calidad*, 1-2

British Standards Institution (BSI). (2006). BS 25999-1 Code of Practice for Business Continuity Management. ReinoUnido: BSI.

British Standards Institution (BSI). (2007). BS 25999-2 Business Continuity Management-Part 2: Specification. Reino Unido: BSI.

British Standards Institution (BSI). (2008). Information and communications technology continuity management. Code of practice. Reino Unido: BSI.

National Institute of Standards and Technology (NIST). (2010). Contingency Planning Guide for Federal Information Systems, Publication 800-34. USA: NIST

Information Systems Audit and Control Association (ISACA). (2011). An Introduction to ICT Continuity Based on BS 25777. Recuperado de https://www.isaca.org/Journal/archives/2011/Volume-2/Pages/An-Introduction-to-ICT-Continuity-Based-on-BS25777.aspx#3 [Consulta: 29 de agosto de 2019].

International Organization for Standardization (ISO) (2012) Sistema de Continuidad de Negocio. ISO/IEC 22301:2012.

International Organization for Standardization (ISO) (2007) Seguridad social: guía para la preparación de incidentes y la gestión de la continuidad operativa. ISO/PAS 22399:2007.

Sharp, J. (2007). The Route Map to Business Continuity Management: Meeting the Requirements of BS 25999: 0. Reino Unido: The British Standards Institution. ISBN: 978-0-580-74341-2.

Hotchkiss, S. (2010). Business Continuity Management: A Practical Guide. Reino Unido: BCS, the Chartered Institute for IT. ISBN: 978-1906124724.

Bello, J. (2008). BS 25999, la nueva norma para Sistemas de Gestión de la Continuidad del Negocio. *AEC: Asociación Española Para La Calidad*, 1-2

International Organization for Standardization (ISO). "s.f" (sin fecha). BSI (United Kingdom). Reino Unido: ISO. Recuperado de https://www.iso.org/member/2064.html [Consulta: 10 de octubre de 2019].

Soluciones Informáticas (Tecnozero). (2019). Gartner DRaaS 2018. Madrid. Recuperado de https://www.tecnozero.com/copia-de-seguridad/gartner-draas-2018/ [Consulta: 15 de octubre de 2019].

Hiles, A., (2004). Bussiness Continuity: Best Practices. Estados Unidos: Rothstein Associates, Inc. ISBN: 978-1931332224

British Standards Institution (BSI) (2018). Gestión de Riesgos ISO 31000. Reino Unido: ISO. Recuperado de https://www.bsigroup.com/es-PE/gestion-de-riesgo-iso-31000-/ [Consulta: 15 de octubre de 2019].

Hellstrom, T. (2009). New vistas for technology and risk assessment? The OECD Programme on Emerging Systemic Risks and beyond. Estados Unidos: Technology in Society.

Pmg-ssi. (ISOTools) (2019). ¿Cómo realizar el análisis de riesgos según la norma ISO 27001?. Recuperado de: https://www.pmg-ssi.com/2019/04/como-realizar-el-analisis-de-riesgos-segun-la-norma-iso-27001/ [Consulta: 19 de noviembre de 2019].

National Institute of Standards and Technology (NIST). (2012). Guide for Conducting Risk Assessments, Publication 800-30. USA: NIST

Ball. R. & Clement (2004). Aggressive Telecommunications Overbooking Ratios. Estados Unidos: Brigham Young University.

9 GLOSARIO

Backbone: Referido a las principales conexiones troncales de una red. Están compuestas de un gran número de routers o dispositivos de red.

Core: en las redes de telecomunicaciones, el término "core o núcleo" es utilizado por los proveedores de servicios y se refiere a las instalaciones de comunicación de alta capacidad que conectan los nodos primarios.

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

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

DDoS: en seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

ISP: son las siglas de Internet Service Provider Proveedor de Servicios de Internet, una compañía que proporciona acceso a Internet.

NAP Perú: Un punto de acceso a la red conformado por operaores de servicio en el perú, donde solo se intercambia tráfico de datos nacional.

NOC: En ingles la deniminación Network Operation Center, es un sitio donde se efectura el control y monitoreo de las redes.

Nodo: en telecomunicación, de forma muy general, un nodo es un punto de intersección, conexión o unión de varios elementos que confluyen en el mismo lugar.

SLA: Un Service Level Agreement (SLA) es un contrato que describe el nivel de servicio que un cliente espera de su proveedor.

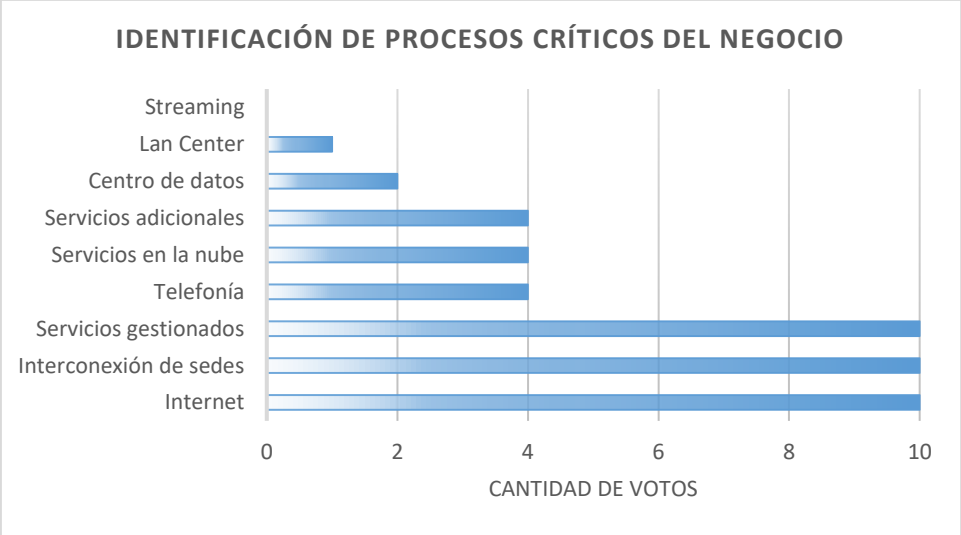
Streaming: es la distribución digital de contenido multimedia a través de una red de computadoras, de manera que el usuario utiliza el producto a la vez que se descarga.

10 SIGLARIO

DRP	Disaster Recovery Plan.
DRI	Disaster Recovery Institute.
TI	Tecnologías de la Información.
BIA:	Business Impact Analysis.
BCI	Business Continuity Institute.
BSI	British Standards Institution.
Gbps	Gigabit por segundo.
NAP	Netwrok Access Point.
MPLS	Multiprotocol Label Switching
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ISP	Internet service provider
NOC	Network Operation Center.
SLA	Service Level Agreetment.
VoIP	Voice over IP
ICT DR	Information and communications technology disaster recovery
ISACA	Information Systems Audit and Control Association.
POC	Probe of Concept

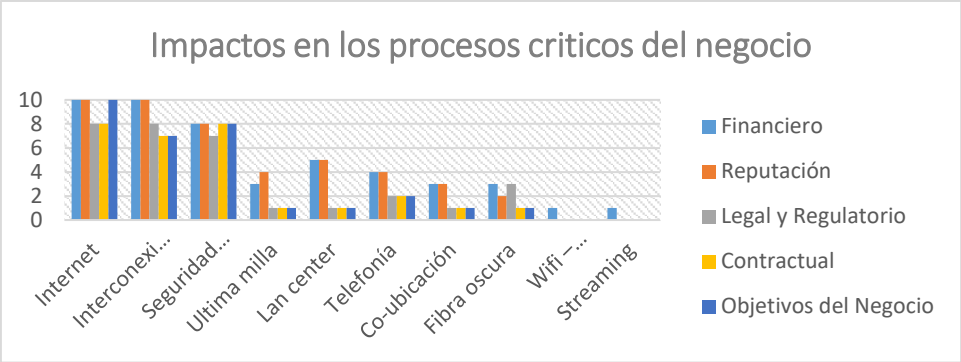
11 ANEXOS

Anexo 1. Cuestionario realizado al personal de la empresa correspondiente al desarrollo del BIA.

Objetivo: Recopilar información esencial del negocio para construir y contrastar datos referentes al BIA
Alcance: Los cuestionarios realizados son relacionados a los procesos del negocio a 10 personas que forman parte de la empresa.
Pregunta 1: ¿De los procesos de negocio que se tiene identificado cuales serían los más críticos? Resultados:    De los 9 procesos identificados solo 3 de ellos tienen los 10 votos de manera unánime por lo que se consideran como procesos críticos los siguientes: • Servicios gestionados. • Interconexión de sedes. • Internet
Pregunta 2: ¿Qué factores definen la criticidad del proceso de negocio? Se identificaron 5 factores que pueden influir en la criticidad del servicio: • Financiero • Reputacional • Legal y regulatorio

- Contractual
- Objetivos del negocio

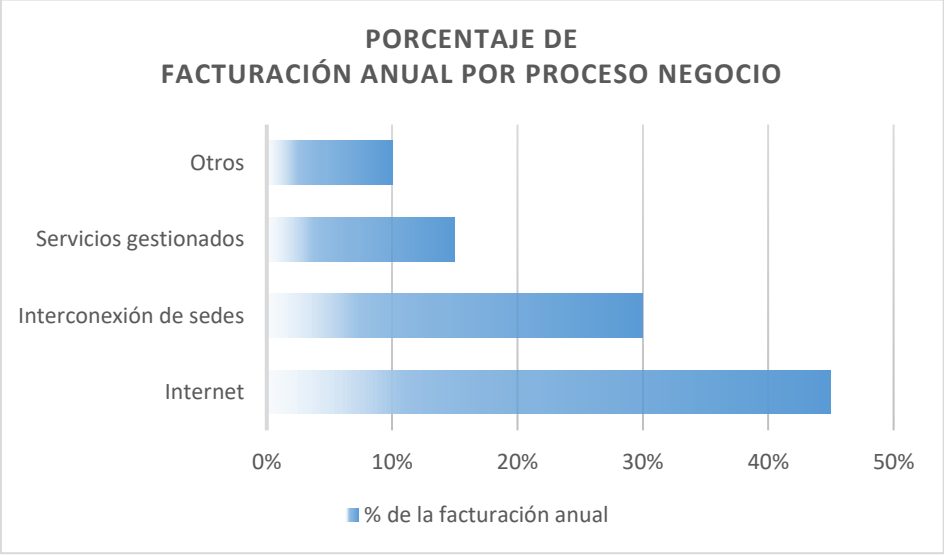
Resultados:



Estos resultados demuestran que los factores que más influyen en los procesos críticos del negocio son Financiero, reputacional y objetivos de negocio. Así mismo se comprueba que los procesos más susceptibles son Internet, Interconexión de sedes y Servicios gestionados.

Pregunta 3: Con respecto al aspecto financiero ¿Cuál es la distribución de los ingresos por proceso de negocio?

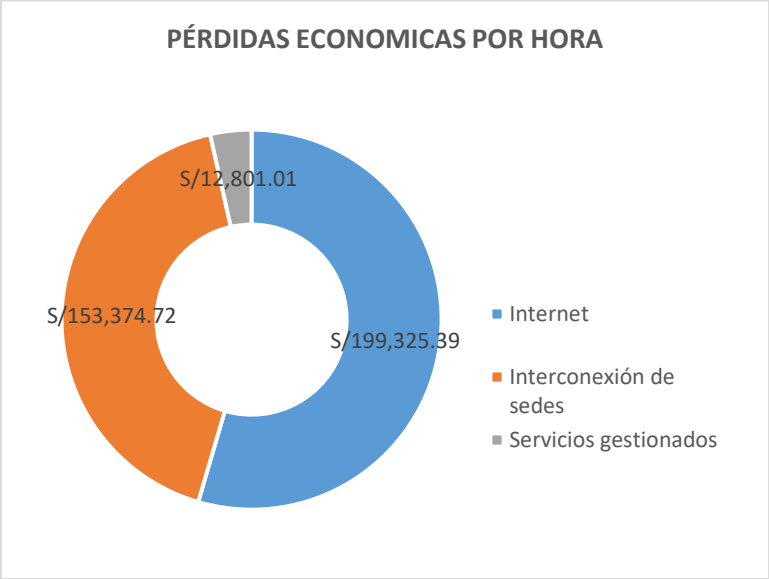
Respuesta:



Según los resultados se puede concluir que el 90% de la facturación anual corresponde a los 3 procesos de negocio Internert, Interconexión de sedes y servicios gestionados.

Pregunta 4: ¿Cuáles son las pérdidas económicas por hora de cada uno de los procesos críticos?

Respuesta:



La información obtenida del área de finanzas define que las pérdidas económicas por hora en caso se presente alguna interrupción.

Pregunta 4: ¿Cuál es el SLA para los procesos críticos del negocio?

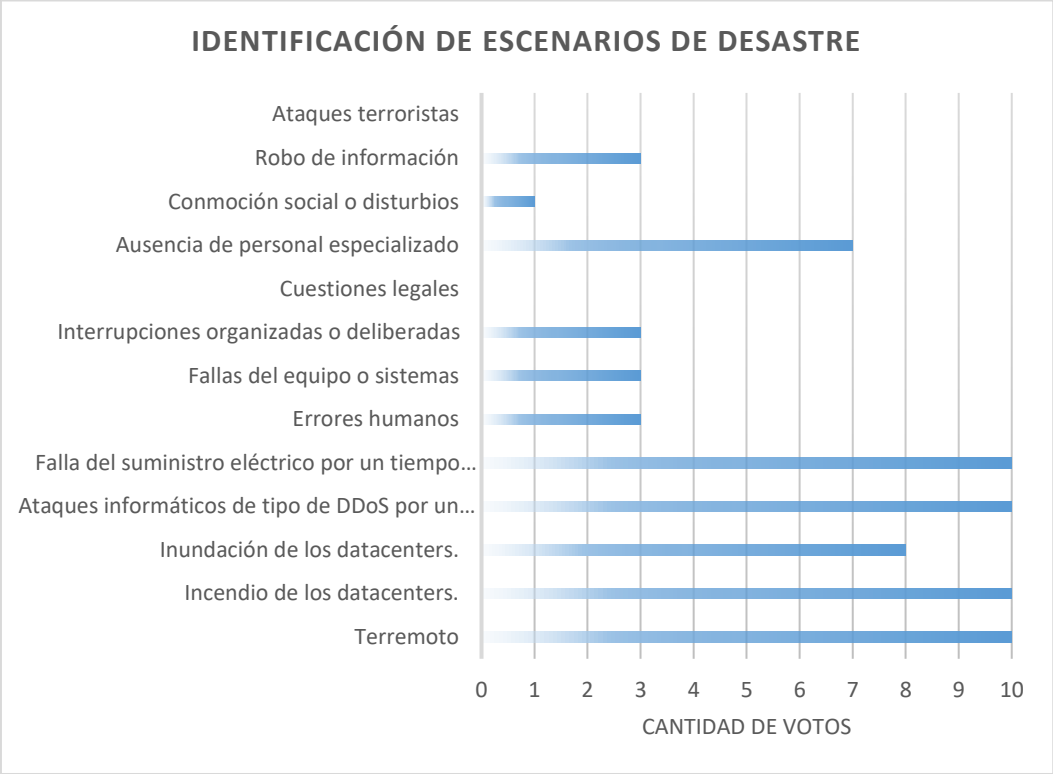
Respuesta:

Como parte de la política de la compañía se ofrece a los clientes los siguientes SLA:

- Internet 99.95%.
- Interconexión de sedes 99.95%.
- Servicios gestionados 99.95%

Pregunta 5: ¿Qué escenarios se catalogarían como desastre para la compañía?

Resultados:

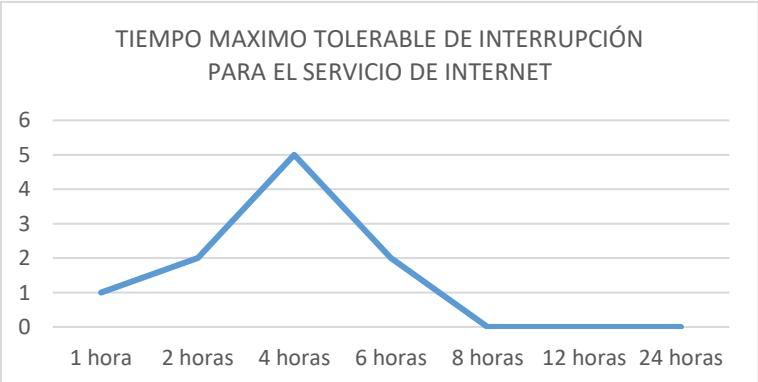


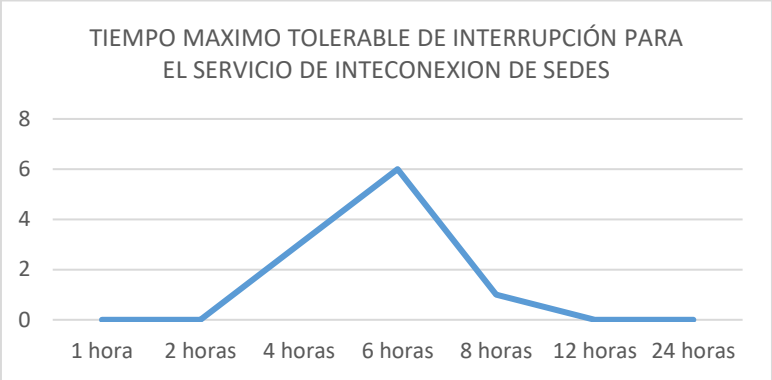
Para esta actividad se identificó los escenarios que podría considerarse un desastre para la compañía, en caso se produjera, para lo cual se realizó un listado de escenario y el personal de la compañía realizó la selección de los escenarios de desastre, siendo los más importantes:

Terremoto, Incendio de los datacenter, Inundación de los datacenter, falla de suministro eléctrico por un tiempo prolongado, Ataques de tipo DDoS, ausencia del personal especializado.

Pregunta 6: ¿Ante un escenario de desastre cual sería el tiempo máximo de interrupción que podría tolerar la compañía?

Resultados:





Para esta actividad se realizó la consulta al personal de la compañía, para determinar el tiempo máximo tolerable de interrupción de cada uno de los procesos críticos del negocio teniendo como resultados:

- Internet 4 Horas
- Interconexión de sedes 6 Horas
- Servicios gestionados 6 Horas

Pregunta 7: ¿Cuáles serían los recursos críticos para el negocio?

Respuesta:

- Equipos de Core de la red metro.
- Equipo de Core de la red MPLs.
- Equipo agregadores.
- Equipo de mitigación de Ataques DDoS.
- Servidores DNS.
- Servidores y herramientas de monitoreo.

• Salas de monitoreo NOC. • Personal.
Pregunta 8: ¿Se tienen controles preventivos para reducir o minimizar los riesgos? Respuesta: Algunos controles implementados son: • Todos los nodos cuentan con sistemas de UPS con autonomía de 2 horas como mínimo. • Los equipos críticos de nodos cuentan con componentes redundantes como Fuentes de poder y tarjetas controladoras. • Se cuentan con sistemas de detección de humo en los datacenters. • Se cuenta con rutas redundantes de fibra óptica para cada nodo. • Se realizan backups automáticos cada 24 horas.

Anexo 2: Manuales y procedimientos

1) Manual de recuperación de backbone DC2
Objetivo: Describir los pasos a seguir para configurar un nuevo equipo de Core en caso de una pérdida total del equipamiento.
Alcance: El alcance de este manual es el proceso de recuperación de equipos de backbone de la capa core correspondiente a la marca Cisco
Procedimiento: Premisa: Este procedimiento se parte desde la premisa de que el equipo de Core ha quedado indisponible. Paso 1: Descargar el ultimo backup de configuración El personal del equipo de respuesta de redes debe de acceder mediante la aplicación Win SCP al servidor de backup 190.12.X.X y descargar el ultimo archivo de configuración del equipo afectado. Paso 2: Retirar el equipo spare de almacén.

El personal del equipo de respuesta debe acceder al almacén y retirar el equipo de spare de acuerdo con el modelo del equipo afectado.

Paso 3: Traslado de personal al sitio

El equipo de respuesta debe trasladarse al sitio donde se presenta la avería con el equipo de spare.

Paso 4: instalación del equipo.

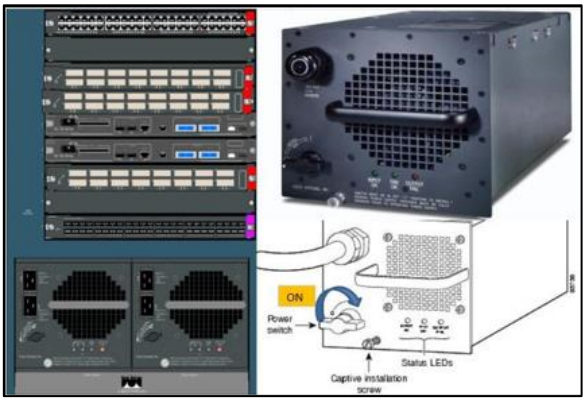
Se debe realizar la instalación del equipo en un rack paralelo a fin de que las conexiones existentes no se confundan o se pierdan.

Antes

Después

Paso 5: Encendido del equipo

En este paso se debe de realizar la energización del equipamiento y encender las fuentes de poder del equipo, con el switch ubicado en la parte inferior.



Paso 6: Cargar la configuración en el equipo.

Conectar el cable consola para poder gestionar el equipo.

Asignar una dirección IP temporal al equipo, realizar una conexión ethernet, activar el servidor TFTP en la laptop y trasladar la configuración mediante el siguiente comando:

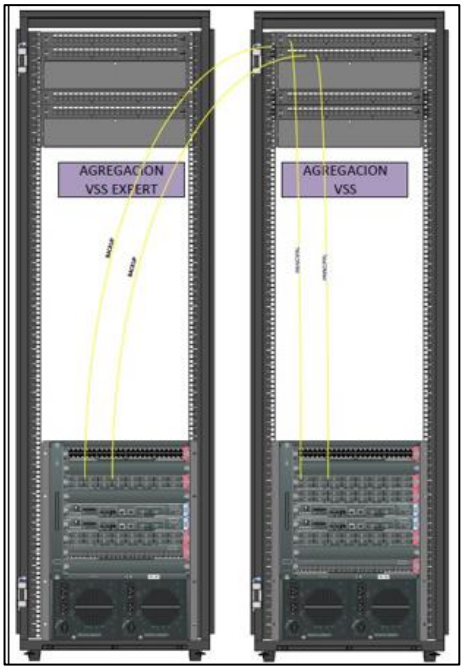
Switch# copy disk0:backup running-config

Al terminar de cargar la configuración se procede a la verificación de manera general

Creación deVlan
Creación de OSPF
Creación de BGP
Creación Interfaces vlan
Creación de Port-Channel

Paso 6: Realizar las conexiones físicas de los cables de F.O

Se debe trasladar las conexiones uno a uno como en la siguiente figura:



Paso 7: Realizar pruebas

Las pruebas a realizar deben ser sobre lo siguiente:

Estado y Adyacencias OSPF
Estado y Sesiones BGP
Estado de Interfaces vlan up|down
Estado de Interface de Port-Channel
Tabla de enrutamiento Total

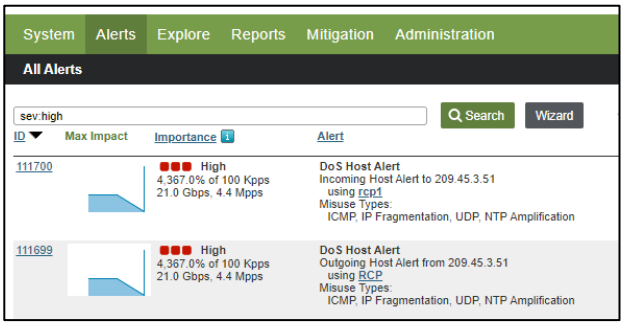
2) Manual de mitigación con Arbor

Objetivo: Describir los pasos a seguir para mitigar ataques de tipo de DDoS

Alcance: El alcance de este manual es el uso correcto del Arbor TMS con una capacidad máxima de 20 Gbps.

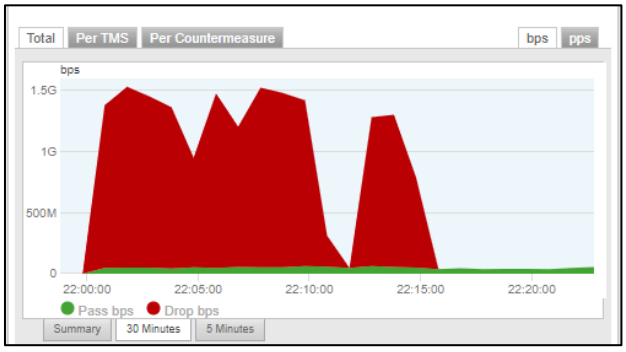
Paso 1: Detección de ataque

Se debe acceder a la herramienta Arbor ya la opción “Alerts”, “All Alerts”



Paso 2: Iniciar la mitigación

Acceder a la opción All mitigations y ejecutar la mitigación



Paso 3: Una vez finalizado la mitigación se debe notificar por correo al área TAC

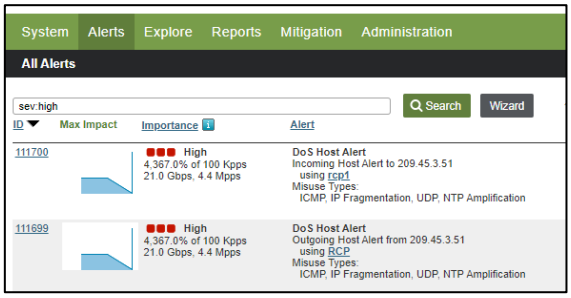
3) Manual de mitigación con blackhole

Objetivo: Describir los pasos a seguir para mitigar ataques de tipo de DDoS mediante un blackhole

Alcance: El alcance de este manual es el uso correcto del Arbor TMS con una capacidad superior a los 20 Gbps.

Paso 1: Detección del ataque

Se debe acceder a la herramienta Arbor ya la opción “Alerts”, “All Alerts”



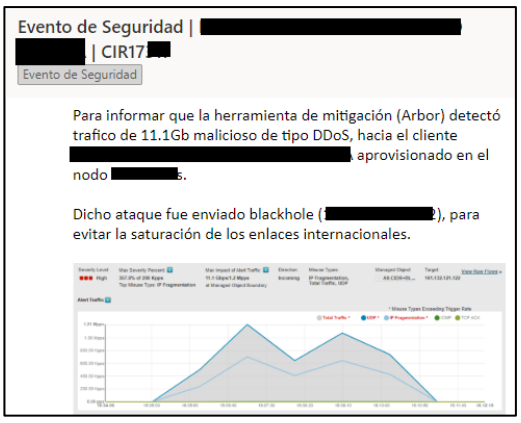
Paso 2: Mitigación con blackhole

Una vez identificado la IP atacada se debe de acceder al router tollgate y realizar la configuración mediante los siguientes pasos:

1. Se configura una ruta null a la ip atacada
2. Se anuncia el prefijo (/32 o /30) en el BGP
3. Se agrega el prefijo en ip prefix-list red_a_telxius_bhr , en una secuencia anterior a la : 80 deny 0.0.0.0/0 le 32

Conf t
Ip route A.B.C.D 255.255.255.255 Null0
router bgp 27843
address-family ipv4
network A.B.C.D mask 255.255.255.255
ip prefix-list red_a_telxius_bhr seq 20 permit A:B:C:D/32

Paso 3: Una vez finalizado la mitigación se debe notificar por correo al área TAC



4) Procedimiento de activación de protocolo de personal especializado externo

Objetivo: Describir los pasos a seguir para el reemplazo del personal especializado por un externo.

Alcance: El alcance de contrato de personal especializado es para las áreas de Redes y Seguridad.

Anexo del Contrato:

ANEXO 02
CATEGORÍA Y ESPECIALIZACIÓN DEL PROFESIONAL

PRIMERA:
EL COMITENTE en calidad de honorarios profesionales por los servicios prestados por EL LOCADOR, pagará la suma bruta de acuerdo con la categoría y especialización, de cada profesional especializado, detallada en la tabla siguiente:

Categoría	Especialización	$ Costo/Mes
Especialista I	Conocimiento y competencias básicas para la gestión de incidencias	$ [redacted]
Especialista II	Conocimiento y competencias intermedias para la gestión de incidencias, problemas y configuración	$ [redacted]
Especialista III	Conocimiento y competencias avanzadas para la gestión de incidencias, problemas, configuración y análisis de reportes.	$ [redacted]

SEGUNDA:
Los pagos se realizarán la primera semana del mes posterior a la entrega del servicio.

Lima, Julio 05 del 2019.

[redacted]

[redacted]

p. El Locador

Paso 1: Establecer comunicación con el proveedor

Se debe establecer comunicación con el proveedor y especificar la especialidad requerida para cubrir temporalmente el puesto.

Paso 2: Asignar roles

Una vez que el personal especializado se haya integrado a la empresa se debe de asignar sus roles, también se debe entregar los manuales y procedimientos correspondientes a sus funciones.