

Prueba de Continuidad del Negocio

Asuntos por tratar

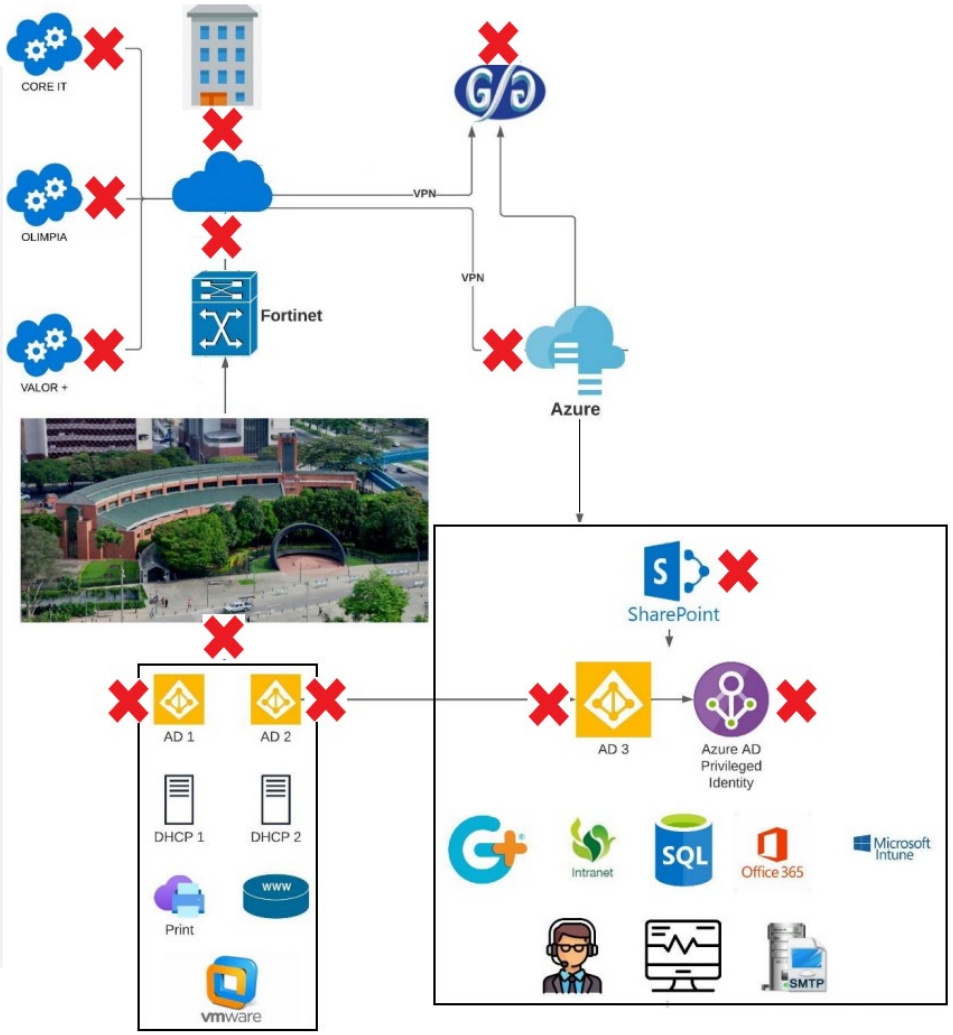
1. Avances y objetivo de la sesión
2. Alternativas de escenarios de desastre a probar
3. Análisis de viabilidad de los escenarios de desastre a probar
4. Riesgos ante alternativas de escenarios de desastre a probar
5. Aprendizajes por considerar para el éxito de las pruebas

1

Avances y objetivo de la sesión

Avances

- Conocimiento de la necesidad e inicio del proyecto.
- Análisis de información documental.
- Validación de información con el área de tecnología.
- Identificación de alternativas de escenarios de desastre a probar.



Objetivo

Acordar escenarios de desastre a probar satisfaciendo las siguientes premisas:

- Efectividad en gestión del riesgo de interrupción de operaciones críticas.
- Cumplimiento de los objetivos de continuidad (RTO, RPO, etc.).
- Alistamiento y disponibilidad de recursos (tecnología, personas, información, instalaciones, suministros procesos) para generar alta probabilidad de éxito de las pruebas.
- Satisfacción de requerimientos y expectativas de la SFC y demás partes interesadas.



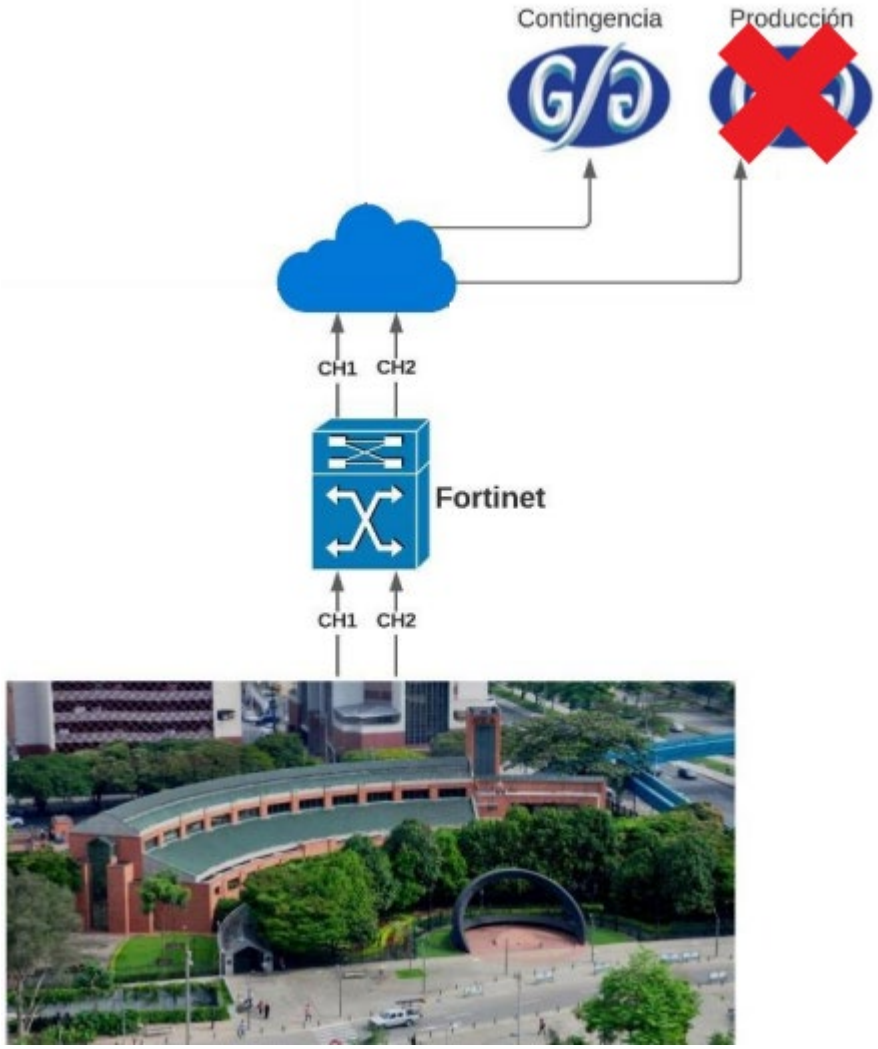
2

Alternativas de escenarios de desastre a probar

Indisponibilidad de servicios a cargo de G & G

Causas: Ciberataques / Falla de canales

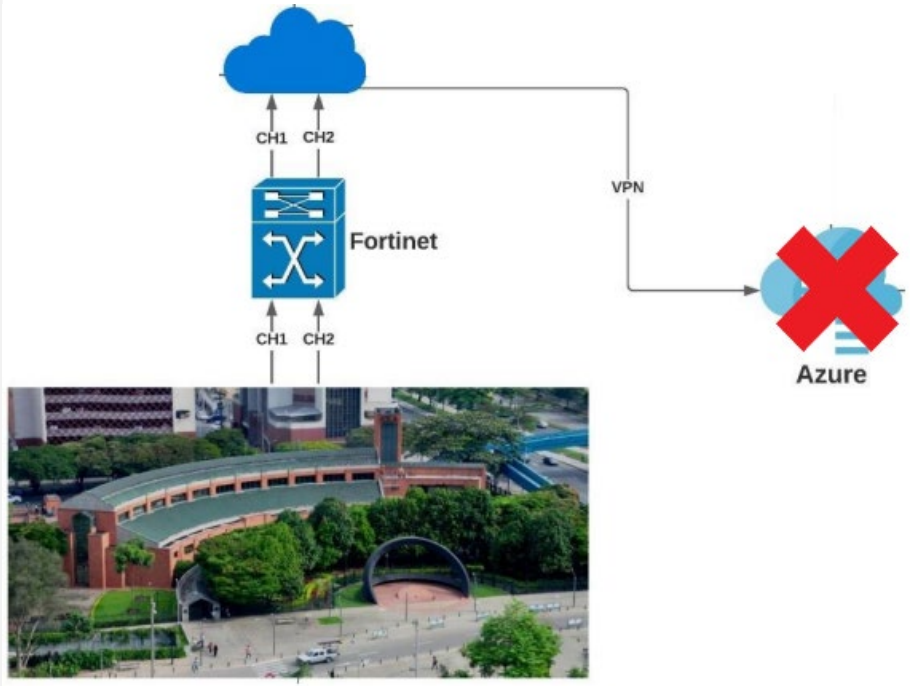
- Comprobar la efectividad del esquema de contingencia establecido en conjunto con el proveedor.
- Establecer si se cumplen los RTO establecidos para los procesos.
- Verificar los esquemas de gestión de crisis y manejo de comunicaciones a partes interesadas.
- Comprobar capacidades tecnológicas para operar en contingencia y efectividad de procedimientos para retorno a la normalidad.
- Servicios de TI afectados: SIIF



Indisponibilidad de servicios de Azure

Causas: Ciberataques / Falla de canales

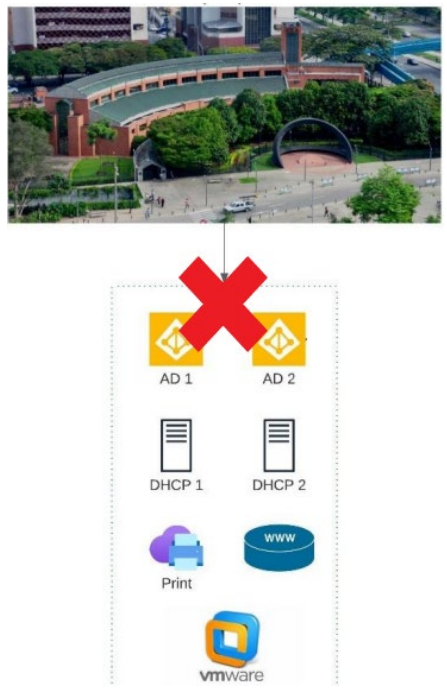
- Comprobar la efectividad de los esquemas de respaldo establecidos para las soluciones y herramientas implementadas en esta nube.
- Establecer si se cumplen los RTO establecidos para los procesos que dependen de estas soluciones y herramientas.
- Verificar los esquemas de gestión de crisis y manejo de comunicaciones a partes interesadas.
- Comprobar capacidades tecnológicas para operar en contingencia y efectividad de procedimientos para retorno a la normalidad.
- Servicios de TI afectados: Sistema de gestión Organizacional G+, intranet, Azure AD, SQL,…



Indisponibilidad del Datacenter On-Premise

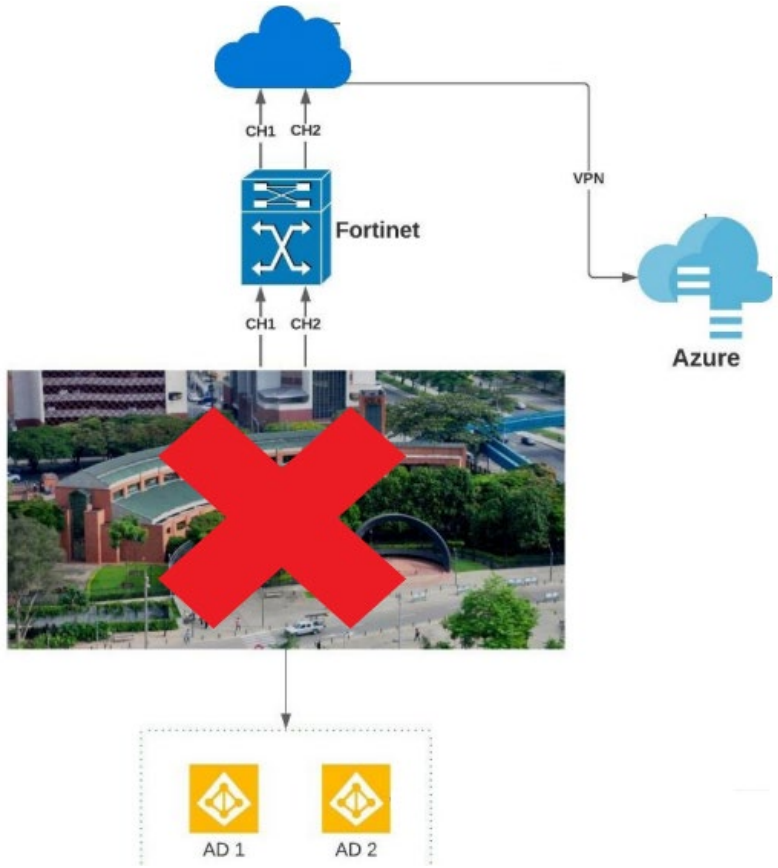
Causas: Ciberataques / Falla de canales

- Comprobar la efectividad de los esquemas de respaldo establecidos para las soluciones y herramientas implementadas en el Datacenter.
- Establecer si se cumplen los RTO establecidos para los procesos que dependen de la infraestructura del Datacenter.
- Verificar los esquemas de gestión de crisis y manejo de comunicaciones a partes interesadas.
- Comprobar las capacidades para la gestión del incidente, la efectividad de los procedimientos establecidos para el antes, durante y después de la contingencia.
- Servicios de TI afectados: Controladores de dominio, DHCP, servicio de impresión, página WEB IDEA, …



Imposibilidad de utilizar instalaciones operativas principales - Causas: Amenazas naturales / Manifestaciones

- Comprobar la debida implementación, alistamiento y disponibilidad de capacidades en el Centro Alterno de Operaciones.
- Comprobar la efectividad de los esquemas de operación desde el Centro Alterno de Operaciones, incluyendo TICs, Información, Personas, Suministros, Instalaciones y Procesos.
- Establecer si se mantiene el cumplimiento de los RTO establecidos para los procesos operando desde el Centro Alterno de Operaciones.
- Verificar los esquemas de gestión de crisis y manejo de comunicaciones a partes interesadas.



3

Análisis de viabilidad de los escenarios de desastre a probar

Establecer las pruebas más viables para ejecutar

- Identificar y acordar aquellas pruebas que tienen mayor viabilidad desde los puntos de vista técnicos y operativos, con la premisa de avanzar de menor a mayor complejidad.
- Definir el plan de trabajo de alistamiento y asignar actividades.
- Establecer recursos, esfuerzos y tiempos necesarios para alistar, ejecutar y documentar las pruebas viables. (Plan de prueba e Informe de prueba).

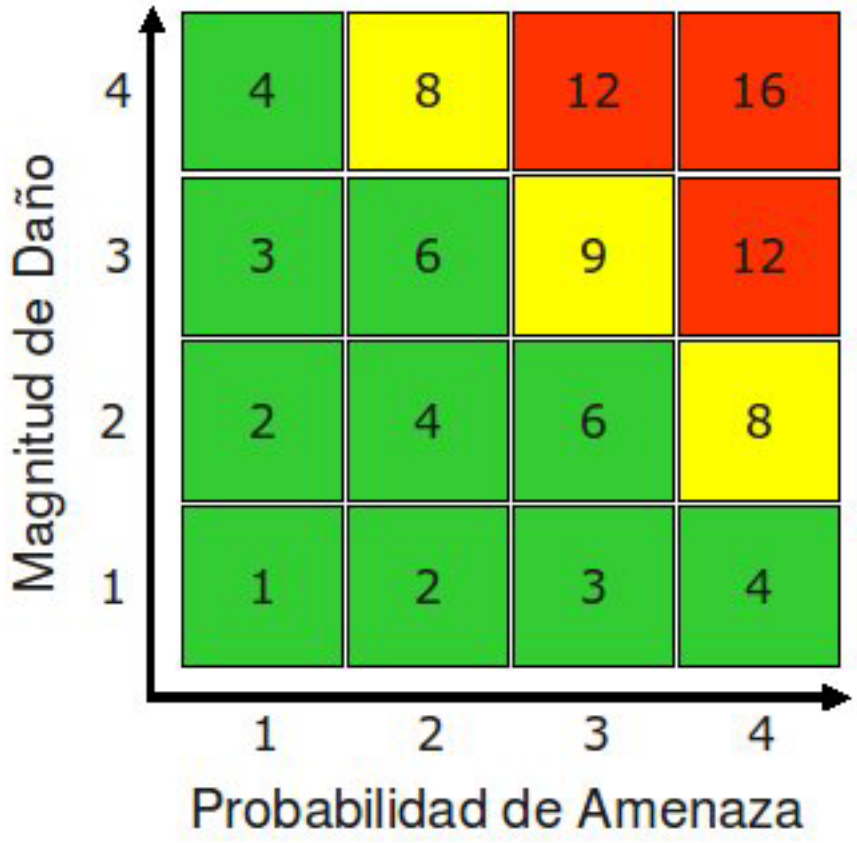


4

Riesgos ante alternativas de escenarios de desastre a probar

Gestionar riesgos ante las pruebas elegidas

- Identificar las situaciones indeseables que pueden presentarse producto del desarrollo de las pruebas elegidas, ej:
  - Afectación real de la operación,
  - Perdida o modificación de datos,
  - Afectación de líneas base de configuración….
- Valorar los impactos que puede generar la materialización de los riesgos
- Definir los controles a implementar o reforzar y asignar actividades pertinentes



5

Aprendizajes por considerar para el éxito de las pruebas

Aprendizajes para considerar

- Identificar, de acuerdo con experiencias previas, aquellas oportunidades de mejora y lecciones aprendidas que requieren ser atendidas antes de la ejecución de las pruebas, ej:
  - Coordinación entre áreas,
  - Copias de respaldo,
  - Conectividad…




IDEA