ANEXO ESPECIFICACIONES TÉCNICAS

Plan de recuperación ante desastres (DRP) para los aplicativos de misión crítica de la Universidad de Cundinamarca.

La Universidad de Cundinamarca actualmente cuenta con un servicio de colocation en un Datacenter Tier III, este es el Datacenter principal donde se alojan todos los servicios WEB, licenciamientos y aplicativos de misión crítica (Plataforma, Pagina WEB, Integradoc), aunque el DataCenter Tier III se encuentra acondicionado para cumplir los requerimientos exigidos por el Uptime Institute, es posible que por razones internaso externas se genere indisponibilidad en los servicios digitales de la Universidad. Con base en esto, a continuación, se relaciona en detalle los requerimientos para implementar un DRP con las capacidades necesarias para la recuperación de los servicios de misión crítica ante cualquier novedad que pueda presentarse.

1. Canal de comunicación

Actualmente la Universidad cuenta con un canal de 100MBPS destinado para el Datacenter principal el cual presenta un porcentaje de uso del 40% en horas pico.

Así mismo, el Datacenter cuenta con un NGFW de Fortigate 1100E en HA por medio del cual es posible establecer un túnel de comunicación (VPN Site to Site) que garantice una comunicación segura y estable, logrando así tener métricas más exactas de consumos y perdidas de comunicación.

Para la solución DRP se requiere:

- Un canal MPLS o VPN S2S de mínimo 15MBPS, para lograr la comunicación entre ambos ambientes: Datacenter principal – DRP. Es importante tener en cuenta que este canal se utilizará para la réplica desde el Datacenter principal hacia la solución DRP garantizando la sincronización de la data, mitigando la pérdida de información en el caso de materializarse un desastre; además, este canal debe servir en vía contraria para sincronizar la información desde el DRP hacia el Datacenter principal cuando éste se logre restablecer después de superada la contingencia. Este canal de comunicación deberá permitir la transferencia bidireccional de datos permitiendo una transferencia mensual de al menos 4TB sin costo

adicional.

- Aprovisionar un esquema de seguridad perimetral dentro de la solución DRP, según las políticas definidas por la institución, este componente de la solución debe brindar los servicios de Firewall, WAF y la facilidad para la configuración de VPN's, configurar las políticas de acuerdo con las indicaciones de la institución.
- Canal de internet de mínimo 40 MBPS para que la comunidad académica pueda acceder a los servicios cuando el DRP se encuentre activo por motivo de la materialización de algún desastre.

2. Seguridad

Para el DRP es requerido contar con un NGFW que permita mantener la seguridad perimetral de los aplicativos WEB en internet, así mismo es requerido la implementación de un WAF para los 3 servicios incluidos en el DRP. Estos servicios deberán ser calculados acorde a los servicios aquí proyectados, para lograr su protección en nube.

3. Requerimientos VM virtualizadas

El alcance del DRP cubre tres (3) servicios de misión crítica como los son, plataforma Institucional, página institucional e integradoc. Estos servicios están soportados por varios servidores virtualizados (VM) de diferentes características, los cuales poseen comunicación específica para lograr la operatividad de las aplicaciones.

Para la solución DRP se requiere contemplar los siguientes servidores virtualizados y físicos que actualmente soportan los 3 servicios que serán contemplados:

Tabla 1, Servidores Virtualizados.

Nombre	S.O.	vCPU	vRAM	VDIS En uso / Asignad		Servicio
sftp_centos x64	CentOS 6.10	4	16GB	380GB	500GB	Plataforma Institucional
tomcat_cen tos6x64	CentOS 6.10	8	40GB	544GB	600GB	
postgress_c entos7x64	CentOS 6.10	4	8GB	34GB	160GB	
portal_cent osx64	CentOS 7.7.1908	8	8GB	500GB	500GB	Página Institucional
Integradoc_ centos7	CentOS 7.7.1908	4	14GB	575GB	900GB	Integradoc

Además, se debe contemplar la base de datos Oracle 12C la cual se encuentra vinculada al servicio de la plataforma institucional. Esta base de datos actualmente se encuentra en un ODA X7-2S On-Premise con un licenciamiento Standard y soporte activo. Por lo anterior, para la solución DRP se requiere el licenciamiento Standar Edition para la base de datos Oracle 12C.

Es necesario aclarar que el servicio de “Pagina Institucional” posee una base de datos MySQL para su funcionamiento y el servicio de “Integradoc” usa una base de datos PostgreSQL, las dos bases de datos están contenidas en su servidor respectivo según la *Tabla 1, Servidores Virtualizados.*

4. Requerimientos Sincronización

La solución DRP debe asegurar:

- La sincronización en tiempo real de los datos de las bases de datos (MySQL, PostgreSQL, Oracle), entre el Datacenter principal y la solución DRP.
- La sincronización periódica y continua de los servidores de aplicaciones entre los ambientes del Datacenter principal y la solución del DRP.
- Permitir la réplica de los ambientes de producción en el ambiente DRP, cuando se realicen actualizaciones de estos ambientes, como: SO, servidores de aplicaciones, aplicativos u otros servicios.
- La sincronización entre el ambiente DRP y el Datacenter principal, cuando se restablezca este último después de presentarse algún desastre.
- Mantener los ambientes operativos y actualizados para minimizar la pérdida de la información.
- RTO: El tiempo objetivo de recuperación debe ser inferior a 2 horas a partir de la materialización de desastre
- RPO: El punto objetivo de recuperación debe ser inferior 30 minutos a partir de la materialización de desastre

Durante la implementación y ejecución del DRP se debe permitir la actualización de los sistemas operativos así como las versiones de los paquetes de software usados para los diferentes aplicativos tanto para las VM's como para las bases de datos, así mismo permitir las actualizaciones y parches de seguridad que apliquen, los cuales son liberados por los soportes de cada servicio según sea la necesidad, esto con la finalidad de lograr una homogeneidad entre los dos ambientes y así garantizar un correctofuncionamiento y sincronización de los datos.

5. Validación de la Solución

- La Universidad solicita la ejecución de pruebas de operación del DRP de manera trimestral, para validar su correcto funcionamiento.
- El oferente deberá entregar informes trimestrales de las pruebas realizadas a través de correo electrónico.
- Se requiere una herramienta de monitoreo para verificar el estado funcional de la solución.

6. Documentación y Capacitación

- El oferente debe entregar la documentación del diseño, la arquitectura, el despliegue y la ejecución del plan de recuperación de desastres.
- En la documentación se debe especificar el procedimiento a seguir para activar la solución DRP en caso de presentarse una contingencia, incluyendo las actividades a ejecutar y los responsables de las mismas, así como la matriz de comunicaciones para el soporte
- También debe incluir el procedimiento para el retorno de las operaciones al ambiente del Datacenter principal de la universidad.

La Universidad requiere que se realice la transferencia de conocimiento de la solución DRP, conceptos técnicos y mejores prácticas a los ingenieros de Servicios Tecnológicos de la Dirección de Sistemas y Tecnología.

7. Atención y Soporte

- Los canales de soporte deben estar disponibles 7x24x365 durante el tiempo de ejecución.
- Deben entregar un matriz de escalamiento del servicio.
- El oferente debe habilitar como mínimo los siguientes canales de atención: línea telefónica, correo electrónico y una mesa de servicio.
- El oferente deberá los ANS que aplicarán durante la ejecución del proyecto.

DANIEL ANDRES ROCHA RAMIREZ
Director Sistemas y Tecnología

PAOLA ANDREA RAMIREZ SUAZA
Profesional Director de Área I
Dirección de Sistemas y Tecnología

LEONARDO MORENO PACHÓN
Profesional Director de Área
Dirección de Sistemas y Tecnología

Transcriptor: Área de Servicios Tecnológicos
15.