ANEXO ESPECIFICACIONES TÉCNICAS AL PROYECTO: "ADQUIRIR LA SOLUCIÓN E IMPLEMENTACIÓN DEL PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP) EN CUANTO A LA INFRAESTRUCTURA TECNOLÓGICA PARA SOPORTAR LOS SERVICIOS DE MISIÓN CRÍTICA DE LA UNIVERSIDAD DE CUNDINAMARCA 2025-2026"

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

La Universidad de Cundinamarca actualmente tiene contratado un servicio de Collocation en un Datacenter Tier III, allí 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 inevitable que por razones internas o externas se genere indisponibilidad en los servicios digitales de la Universidad. Con base en esto, se relaciona a detalle los requerimientos para implementar un DRP capaz de respaldar al sitio principal, con la posibilidad de responder las solicitudes de los procesos de misión critica identificados.

1. Canal de comunicación

Con la finalidad de lograr una comunicación bidireccional entre el DataCenter de la Universidad y el DRP, actualmente la Universidad cuenta con un canal de 100MB destinado para el uso exclusivo de DataCenter el cual tiene un porcentaje de uso del 40% en horas pico. Para el DRP es requerido contar con un canal de 15MB para lograr la comunicación entre ambos ambientes. Actualmente contamos con un NGFW 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.

Este canal de comunicación deberá permitir la transferencia bidireccional de datos permitiendo una transferencia mensual de al menos 4TB sin costo adicional, que permita asegurar la sincronización entre el DRP y la infraestructura de la Universidad.

2. Seguridad y salas de control

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.

3. Requerimientos VM virtualizadas

El alcance del DRP cubre a 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.
Es por lo que a continuación se listan los servidores virtualizados y físicos que se verán afectados:

Tabla 1, Servidores Virtualizados.

Nombre	S.O.	vCPU	vRAM	vDISK En uso / Asignado		Servicio
Plataforma Academusoft (SI)	Oracle Linux 8.6	8	20GB	225GB	500GB	Plataforma Institucional
Plataforma Gestasoft (SI)	Oracle Linux 8.6	8	40GB	544GB	600GB	
Plataforma HTTP (SI)	Oracle Linux 8.6	4	4GB	84GB	500GB	
Plataforma Aplicaciones propias (SI)	Oracle Linux 8.6	8	36GB	16GB	500GB	
Plataforma Server-NFS (SI)	Oracle Linux 8.6	2	4GB	241GB	1.24TB	
Plataforma postgres producción (SI)	Oracle Linux 8.6	4	8GB	35GB	160GB	
postgress_centos7x64	Oracle Linux 8.6	4	8GB	34GB	160GB	
portal_centosx64	CentOS 7.7.1908	4	8GB	200GB	500GB	Pagina Institucional
Integradoc-AppServer	Ubuntu Server 20.04.6 LTS	4	16GB	100GB	250GB	Integradoc
Integradoc-DBServer	Ubuntu Server 24.04 LTS	4	8GB	600GB	1TB	

Adicional a estos servidores se debe contemplar la vinculación de la DB Oracle 19 la cual se encuentra vinculada al servicio de la plataforma institucional. Esta DB actualmente se encuentra en un ODA X7-2S On-Premise con licenciamiento y soporte activo. Es necesario realizar la sincronización continua de la DB entre el DRP y la infraestructura privada de la Universidad de Cundinamarca, para garantizar la correcta funcionalidad de las aplicaciones evitando la perdida de la información.

4. Objetivos de Recuperación (RTO y RPO)

Para los servicios de misión crítica de la Universidad de Cundinamarca se definen los siguientes parámetros:

Servicio	Tiempo máximo aceptable de recuperación (RTO)	Pérdida máxima de datos permitida (RPO)
Plataforma Institucional (Academusoft / Gestasoft / aplicaciones propias)	4 horas	15 minutos
Página Web Institucional	2 horas	30 minutos
Integradoc	4 horas	15 minutos

- **RTO (Recovery Time Objective)**
  Tiempo máximo aceptable para restablecer la operación del servicio después de un desastre.

- **RPO (Recovery Point Objective)**
  Cantidad máxima de datos que se pueden perder medida en tiempo.

Estos valores se logran mediante:

- Replicación continua de máquinas virtuales.
- Sincronización periódica de repositorios.
- Replicación de base de datos Oracle.
- Respaldos automatizados mediante Veeam Backup & Replication.

5. Prioridades de Recuperación de Servicios

En caso de activación del DRP, los servicios serán restaurados en el siguiente orden de prioridad:

Prioridad	Servicio	Justificación
Alta	Página Web Institucional	Portal informativo y acceso a servicios
Alta	Base de datos Oracle (ODA)	Requerida para el funcionamiento de la Plataforma Institucional

Media	Plataforma Institucional	Soporta los procesos académicos y administrativos principales de la Universidad
Media	Integradoc	Gestión documental institucional

6. Escenarios de Desastre Contemplados

Se definen los siguientes escenarios de desastre que pueden afectar la disponibilidad de los servicios digitales institucionales.

6.1. Caída total del Datacenter principal

Qué se afecta

- Plataforma Institucional
- Página Web Institucional
- Integradoc
- Bases de datos Oracle (ODA)
- Servicios virtualizados en la solución de hiperconvergencia Nutanix

Activación del DRP

- Validación de indisponibilidad del sitio principal.
- Declaración de incidente mayor por el área de Servicios Tecnológicos.
- Activación del ambiente DRP en el sitio alterno.
- Encendido de las máquinas virtuales replicadas.

Servicios que se recuperan primero

1. Base de datos Oracle (ODA)
2. Plataforma Institucional
3. Integradoc
4. Página Web Institucional

6.2. Ataque de Ransomware

Qué se afecta

- Servidores virtualizados en la solución de hiperconvergencia Nutanix
- Repositorios de almacenamiento
- Bases de datos
- Sistemas operativos

Activación del DRP

- Aislamiento inmediato de la infraestructura afectada.
- Análisis del incidente por el equipo de seguridad.
- Restauración de servidores desde respaldos inmutables.
- Validación de integridad de los datos restaurados.

Servicios que se recuperan primero

1. Página Web Institucional
2. Base de datos Oracle (ODA)
3. Plataforma Institucional
4. Integradoc

6.3. Falla eléctrica prolongada

Qué se afecta

- Infraestructura física del Datacenter
- Equipos de red
- Servidores físicos
- Sistemas de almacenamiento

Activación del DRP

- Verificación de falla prolongada en el sitio principal.
- Activación de replicación hacia el sitio alterno.
- Encendido de máquinas virtuales en el DRP.

Servicios que se recuperan primero

1. Plataforma Institucional
2. Integradoc
3. Página Web

6.4. Falla de comunicaciones

Qué se afecta

- Acceso externo a servicios web
- Comunicación entre sedes
- Acceso a aplicativos institucionales

Activación del DRP

- Redirección del tráfico al sitio alterno.
- Activación de rutas de comunicación redundantes.
- Validación de conectividad con usuarios finales.

Servicios que se recuperan primero

1. Página Web
2. Plataforma Institucional
3. Integradoc

6.5. Error humano

Qué se afecta

- Eliminación accidental de datos
- Configuración errónea de servidores

- Fallas en bases de datos

Activación del DRP

- Identificación del incidente.
- Restauración de información desde backups.
- Validación de integridad de datos.

Servicios que se recuperan primero

1. Base de datos afectada
2. Aplicaciones asociadas
3. Servicios dependientes

6.6. Desastre natural

Qué se afecta

- Infraestructura física
- Equipos del Datacenter
- Conectividad

Activación del DRP

- Declaración oficial de desastre.
- Activación total del DRP.
- Encendido de infraestructura virtual en el sitio alterno.

Servicios que se recuperan primero

1. Plataforma Institucional
2. Integradoc
3. Página Web

7. Procedimiento General de Activación del DRP

El DRP se activará bajo las siguientes condiciones:

- Confirmación de indisponibilidad del servicio superior al RTO definido.
- Evaluación del incidente por la Dirección de Sistemas y Tecnología.
- Declaración de contingencia.
- Activación de máquinas virtuales en el sitio alterno.
- Validación de funcionamiento de servicios.
- Comunicación oficial a los usuarios institucionales.

8. Pruebas periódicas del Plan de Recuperación ante Desastres (DRP)

Con el fin de garantizar la efectividad del Plan de Recuperación ante Desastres (DRP), el proveedor deberá realizar pruebas periódicas de recuperación que permitan

validar la operatividad de los respaldos, la replicación de datos y la capacidad de recuperación de los servicios críticos.

8.1. Tipos de pruebas
8.1.1. Prueba de restauración de respaldos

Se realizará la restauración de máquinas virtuales o archivos específicos a partir de respaldos almacenados en el repositorio de copias de seguridad.

Objetivo:
- Verificar la integridad de los respaldos.
- Validar tiempos de restauración.
- Comprobar la disponibilidad de la información.

Frecuencia mínima: trimestral

8.1.2. Prueba de recuperación parcial
Se simulará la caída de uno de los servicios críticos para validar la recuperación en el sitio alterno.

Objetivo:
- Validar la activación del DRP.
- Verificar el funcionamiento de máquinas virtuales replicadas.
- Evaluar tiempos de recuperación frente a los RTO definidos.

Frecuencia mínima: semestral

8.1.3. Prueba de recuperación total del sitio

Se realizará un ejercicio controlado que simule la indisponibilidad total del Datacenter principal.

Objetivo:
- Validar la operación completa desde el sitio DRP.
- Confirmar el orden de recuperación de los servicios.
- Evaluar los procedimientos de comunicación institucional.

Frecuencia mínima: anual

8.1.4. Reportes de pruebas

Cada prueba deberá generar un informe técnico que incluya:
- Fecha de ejecución
- Servicios probados
- Tiempo real de recuperación (RTO alcanzado)

- Integridad de datos recuperados (RPO alcanzado)
- Hallazgos identificados
- Acciones de mejora

Estos reportes deberán ser entregados mediante informe técnico al correo de la **Dirección de Sistemas y Tecnología de la Universidad de Cundinamarca (sistemasytecnologia@ucundinamarca.edu.co),** con copia al correo del **Área de Servicios Tecnologicos (serviciostecnologicos@ucundinamarca.edu.co).**

9. Arquitectura técnica del Plan de Recuperación ante Desastres (DRP)

La solución de recuperación ante desastres deberá basarse en una arquitectura de replicación y respaldo que garantice la disponibilidad de los servicios críticos institucionales.

9.1. Componentes principales

9.1.1. Plataforma de virtualización

La infraestructura de los servicios institucionales se encuentra virtualizada sobre plataforma Nutanix, por lo cual el DRP deberá permitir:

- Replicación de máquinas virtuales.
- Restauración directa en ambientes VMware.
- Recuperación completa de servidores virtualizados.

9.1.2. Plataforma de respaldo

La solución deberá utilizar Veeam Backup, permitiendo:

- Copias de seguridad automáticas.
- Replicación de máquinas virtuales.
- Restauración granular de archivos y servidores.
- Monitoreo de respaldos.
- Reportes de estado.

9.1.3. Repositorio de respaldos

El servicio deberá incluir:

- **20 TB de almacenamiento en nube**
- Repositorios seguros para respaldos
- Protección contra corrupción de datos
- Capacidad de restauración parcial o total

9.1.4. Replicación de bases de datos

La base de datos **Oracle 19 alojada en ODA X7-2S** deberá contar con mecanismos de sincronización hacia el ambiente DRP que permitan:

- Replicación continua
- Consistencia de datos
- Reducción de pérdida de información

9.1.5. Conectividad entre sitios

La comunicación entre el Datacenter principal y el sitio DRP deberá establecerse mediante:

- VPN Site-to-Site
- Canal dedicado mínimo de 15 Mbps
- Transferencia mensual mínima de 4 TB

Este canal permitirá la sincronización continua entre los ambientes.

9.1.6. Seguridad

El sitio DRP deberá contar con los siguientes mecanismos de seguridad:

- NGFW (Next Generation Firewall) para protección perimetral
- WAF (Web Application Firewall) para los aplicativos web
- Segmentación de red
- Políticas de acceso seguro

10. Monitoreo y operación del DRP

El servicio deberá incluir monitoreo permanente de la plataforma de respaldo y recuperación.

10.1. Alcance del monitoreo (El monitoreo deberá operar 7x24)

- Estado de respaldos
- Replicación de máquinas virtuales
- Uso de almacenamiento
- Disponibilidad del repositorio
- Estado de restauraciones

10.2. Gestión de incidentes

El proveedor deberá atender incidentes relacionados con:

- Fallas en respaldos
- Errores en replicación
- Problemas de restauración
- Fallas en repositorios

La atención se realizará mediante:

- Soporte telefónico
- Soporte web
- Atención bajo demanda

11. Acuerdos de Nivel de Servicio (SLA)

El proveedor del servicio deberá garantizar niveles de disponibilidad y tiempos de atención que permitan asegurar la continuidad de los servicios de misión crítica de la Universidad de Cundinamarca.

11.1. Disponibilidad del servicio

El servicio de respaldo, replicación y recuperación deberá garantizar una disponibilidad mínima mensual de:

99.98 % de disponibilidad del servicio

Este nivel de disponibilidad aplica para:

- Plataforma de respaldos
- Infraestructura del repositorio
- Servicios de monitoreo
- Plataforma de recuperación ante desastres

11.2. Tiempos de respuesta

Los tiempos de atención ante incidentes deberán ajustarse a los siguientes niveles:

Nivel de incidente	Descripción	Tiempo máximo de respuesta	Tiempo máximo de solución
Crítico	Caída total de servicios de misión crítica	30 minutos	4 horas
Alto	Degradación significativa del servicio	1 hora	8 horas
Medio	Fallas parciales o errores operativos	4 horas	24 horas
Bajo	Solicitudes de configuración o ajustes menores	8 horas	48 horas

11.3. Disponibilidad de soporte

El proveedor deberá garantizar:

- Soporte técnico 7x24
- Atención telefónica y web
- Escalamiento técnico especializado
- Atención de incidentes críticos fuera de horario laboral

12. Niveles de severidad de incidentes

Para efectos de la gestión de incidentes asociados al servicio de respaldo y recuperación, se establecen los siguientes niveles de severidad.

12.1. Severidad crítica (Sev-1)

Corresponde a incidentes que generan indisponibilidad total de servicios institucionales.

Ejemplos:

- Caída total del Datacenter
- Imposibilidad de restaurar respaldos
- Fallas críticas en repositorios de respaldo
- Pérdida de replicación entre sitios

Impacto: Afectación directa a los procesos académicos, administrativos o institucionales.

Acción requerida:

- Activación inmediata del DRP
- Atención prioritaria
- Escalamiento inmediato al proveedor

12.2. Severidad alta (Sev-2)

Corresponde a incidentes que generan degradación significativa del servicio.

Ejemplos:

- Fallas en replicación de máquinas virtuales
- Errores en tareas de respaldo
- Problemas en repositorios de almacenamiento
-

Impacto: Riesgo potencial sobre la disponibilidad o integridad de los datos.

Acción requerida:

- Diagnóstico inmediato
- Corrección prioritaria
- Validación de integridad de datos
-

12.3. Severidad media (Sev-3)

Corresponde a incidentes que afectan parcialmente la operación.

Ejemplos:

- Fallas en reportes de monitoreo
- Problemas menores en configuración
- Alertas de advertencia en respaldos

Impacto: No afecta directamente la operación institucional.

Acción requerida:

- Corrección programada
- Seguimiento técnico

12.4. Severidad baja (Sev-4)

Corresponde a solicitudes de servicio o ajustes operativos.

Ejemplos:

- Ajustes en políticas de respaldo
- Configuración de usuarios
- Cambios en programación de respaldos
- Solicitud de reportes

Impacto: Sin impacto en la disponibilidad del servicio.

Acción requerida:

- Atención dentro de los tiempos establecidos.

CAROLINA SANCHEZ BARRERA
Profesional IV
Dirección de Sistemas y Tecnología
Universidad de Cundinamarca

Proyecto: Ing. Carolina Sánchez
Área Servicios Tecnológicos