INGENIERIA DE SISTEMAS – SPTI 2021-1

LABORATORIO 5:

Realización de DRP

GERSON DAVID QUINTERO RODRIGUEZ

Autor:

Torres Segura Duck James Alexander

Jimmy Armando Chirivi Nivi

1. INFORME GENERAL

1.1. OBJETIVO GENERAL

Realizar un análisis y elaboración de un plan de trabajo para poder mantener la infraestructura de la empresa en el caso de haber un evento de interrupción mayor como un desastre natural o un daño físico.

1.2. RESPONSABLE

Arquitecto de infraestructura, Arquitecto de Software y Lideres de área de Desarrollo.

1.3. ALCANCE

A continuación, se especificará las plataformas y aplicaciones tecnologías que soportan la infraestructura de la empresa:

Tipo de Componente	Descripción	Tipo de Tolerancia
Aplicaciones	- Gestor Financiero - Gestor de versionamiento local	- 12 horas - 24 horas
Mesajeria	- Correo electrónico	- 12 horas
Comunicaciones	- Infraestructura de Internet - Enlace Cloud	- 24 horas - 12 horas
Infraestructura	- Servidores locales de almacenamiento - UPS	- 24 horas - 8 horas

Tabla 1: Componentes y sistemas

1.4. DEFINICIONES

BCP: Sigla en inglés (Business Continuity Plan) que hace referencia al Plan de Continuidad de Negocio, el cual integra el DRP, planes de contingencia y recuperación de procesos de la
entidad, planes de emergencia, y plan de comunicación y administración de crisis.

BIA: Sigla en inglés (Business Impact Analisys), y hace referencia a un documento que identifica la disponibilidad requerida de la plataforma tecnológica para soportar los procesos de la entidad, con el fin de garantizar la continuidad en la prestación del servicio a
los usuarios internos y externos.

DRP: Sigla en inglés (Disaster Recovery Plan), que hace referencia al Plan de Recuperación ante Desastres de Tecnología, el cual define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

ERA: Sigla en inglés (Environment Risk Analisys), Análisis de Riesgos Ambientales en español, y hace referencia a un documento que relaciona los riesgos que pueden afectar la continuidad de la plataforma tecnológica de la entidad.

RAS: Sigla en inglés (Response Alternative and Solutions), y hace referencia a un documento que relaciona las diferentes alternativas y estrategias potenciales para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

RPO: Sigla en inglés (Recovery Point Objetive), que corresponde a la cantidad de datos o información, en términos de tiempo, que tolera perder un proceso o servicio.

RTO: Sigla en inglés (Recovery Time Objetive), que corresponde al tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.

PLATAFORMA TECNOLÓGICA CRÍTICA: Hace referencia a los sistemas de información, servidores, bases de datos, sistemas de almacenamiento y

respaldo, equipos y enlaces de comunicación que son críticos para soportar los procesos y servicios de la entidad.

2. CONDICIONES GENERALES

2.1. Enfoque

El DRP está enfocado a la protección tecnológica que protege los ambientes tecnológicos y procesos que permiten a la compañía realizar su misión sin descuidar aspectos de inspección, vigilancia y control.

2.2. Supuesto

El DRP tiene como función tener un plan de emergencias para la protección de los ambientes tecnológicos de la organización para poder controlar y vigilar los procesos tecnológicos

- Se implementa un sito alterno y copias de seguridad en servicios de la nube como Azure y AWS.
- Se realizan copias de seguridad de bases de datos en servidores locales de otra ubicación y en la nube
- En caso de contingencia se realiza trabajo remoto con conexión a servidores en la nube
- Los líderes de áreas son los responsables de ejecutar el plan de contingencia tecnológico para no perder los tiempos de gestión de los proyectos.

3. GUIA DEL PLAN DE RECUPERACIÓN ANTE DESASTRES

3.1. ESCENARIO DE DESASTRE

Los escenarios de desastre son las situaciones de contingencia mayor y que se contemplan en esta guía son:

3.1.1. Centro de cómputo:

Ilustración 1: desastre en centro de cómputo

No disponibilidad del centro de cómputo debido a:

- Movimientos sísmicos
- Incendios
- Alta tensión en los Equipos
- Inundación

3.1.2. Infraestructura de Comunicaciones:

Ilustración 2: desastre en la infraestructura de comunicaciones

No disponibilidad de los servicios de comunicaciones por fallas en:

- Switches
- Routers
- Access Point
- Firewall
- SAN
- UPS
- Cable UTP, Coaxial y Fibra óptica

3.1.3. Infraestructura de Servidores:

Ilustración 3: desastre en la infraestructura de servidores

No disponibilidad de los servicios de comunicaciones por fallas en:

- Servidores
- Servidores virtuales

3.1.4. Infraestructura de Bases de datos, Almacenamiento y respaldo

Ilustración 4: desastre en la base de datos de respaldo

No disponibilidad de la información por fallas en:

- El servidor de respaldo
- Conexión con falla total o parcial a la SAN
- Switch con conexión SAN
- Borrado o perdida de información de la base de datos
- Corrupción de la base de datos

CUALQUIER ESCENARIO NO MENCIONADO ANTERIORMENTE, NO HA SIDO CONSIDERADO EN EL PRESENTE DOCUMENTO GUÍA

3.2. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades definidos en este plan solo serán para personal seleccionado de tal forma para reducir el impacto y la mejor actuación ante un evento de forma adecuada.

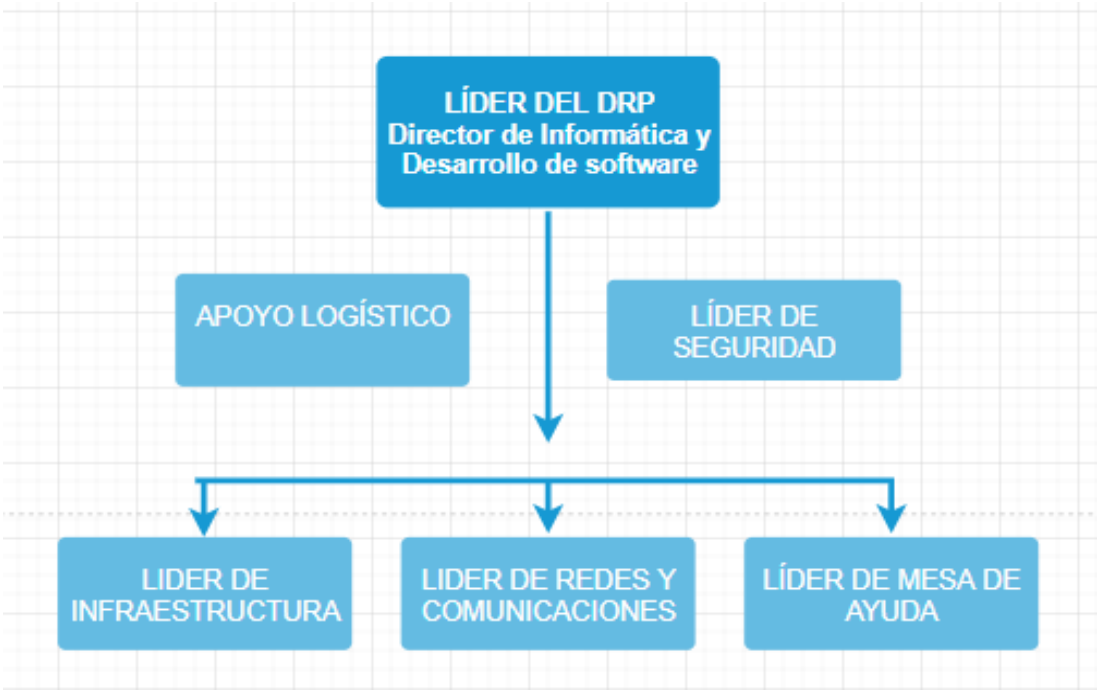

Ilustración 5: Roles

Las responsabilidades para cada rol son el siguiente:

ROL	ANTES DEL EVENTO DE INTERRUPCIÓN	DURANTE DEL EVENTO DE INTERRUPCIÓN	DESPUES DEL EVENTO DE INTERRUPCIÓN
LÍDER DEL DRP	- Velar por la actualización del DRP y los recursos utilizados. - Velar por la actualización y	- Evaluar y activar el DRP con sus estrategias de recuperación y contingencia.	- Velar por la actualización del DRP acorde con los inconvenientes vistos y los recursos utilizados.

	pruebas de la DRP. - Gestionar los recursos de DRP. - Comunicar a las personas sobre la situación de contingencia.	- Comunicar al Secretario General sobre el estado de la operación. - Informar el momento en que opera en contingencia. - Comunicar a la dirección el desastre, interrupción o evento. - Liderar el retorno a la normalidad.	- Informar al Secretario General sobre el retorno a la normalidad y agradecer la comprensión y apoyo de todos en esta situación.
APOYO LOGÍSTICO	- Participar en la ejecución de las pruebas DRP.	- Apoyar a los involucrados en el DRP. - Suministro de información de contrato. - Logística y contacto si es requerido.	- Reportar los inconvenientes Y oportunidades de mejora del DRP.
LÍDER DE SEGURIDAD	- Coordinar actividades de entrenamiento, documentación y actualización del DRP. - Identificar los recursos requeridos para la operación del DRP.	- Proveer soporte a los profesionales especializados. - Gestionar el alistamiento y disponibilidad del Centro de Cómputo.	- Actualizar el DRP, de acuerdo con los Inconvenientes y oportunidades de mejora encontrados.

		- Mantener informado al Líder.	
LIDER DE INFRAESTRUCTURA	- Participar en la ejecución de las pruebas al DRP.	- Evaluar el desastre, interrupción. - En caso de no contar con un contrato de mantenimiento vigente se debe tener un listado de posibles acciones correctivas. - Comunicar el evento al Líder del DRP. - Notificar al personal para atender el evento.	- Reportar los inconvenientes Y oportunidades de mejora del DRP.
LIDER DE REDES Y COMUNICACIONES			
LÍDER DE MESA DE AYUDA			

Tabla 2: responsabilidades

3.3. ACTIVIDADES DE NOTIFICACIÓN, EVALUACIÓN Y ACTIVACIÓN DEL DRP

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

- No se puede utilizar los productos desarrollados.

- No hay acceso a los archivos centralizados.
- No hay red de comunicación.
- No hay acceso a los datos de la base de datos.
- No hay respuesta de los servidores.

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

- Hay un sismo de cualquier escala.
- Hay una inundación en cualquier sector.
- Hay un incendio en cualquier sector.
- Se una las alarmas de seguridad.
- Se activa alarmas de humo en el centro de seguridad.
- Se activa las alertas de los Firewall.

3.3.3. La mesa de ayuda debe atender el incidente de acuerdo con lo establecido en el Procedimiento definido para Mantenimiento preventivo, correctivo y soporte técnico, y se continúa con la ejecución de esta guía si:

- El incidente afecta la disponibilidad de los sistemas.
- El incidente afecta la disponibilidad de la red de comunicaciones a nivel general.
- Ningún usuario tiene acceso a su software.
- Ningún usuario tiene acceso a sus datos en sus bases de datos.

3.3.4. El profesional especializado de la plataforma afectada debe realizar un diagnóstico sobre el incidente presentado, teniendo en cuenta:

- La naturaleza e impacto.
- Estrategias usadas y soluciones potenciales.
- Solución.
- Tiempo.
- Resultado de diagnóstico.

3.3.5. El Jefe de Informática y Sistemas, define si se activa o no el Centro de cómputo Alterno (Azure), teniendo en cuenta los siguientes aspectos:

- Se verifica la afectación al centro de cómputo principal.
- Se clasifica y gestiona la afectación del centro del cómputo principal.
- Se verifica el tiempo de solución utilizado.

3.3.6. En caso de que se active, se debe comunicar la activación al proveedor, teniendo en cuenta:

- Fecha, Hora, Día, Lugar desde el inicio del plan.
- Los permisos de acceso a funcionarios de la entidad.

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

- Enrutamiento y activación de las comunicaciones hacia el centro de cómputo.
- Detección de datos duplicados.
- Verificación de disponibilidad de datos.
- Activación de servidores.
- Activación de base de datos.

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

- acceder a los sistemas de información.
- realizar pruebas sobre los sistemas de información.

3.3.9. El Jefe de Informática y Sistemas, define si comunica o no el incidente a la Alta Dirección, caso en el cual se realizarían las actividades de manejo de crisis.

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

3.3.10.1. Si es un evento que afectó las comunicaciones.

- Configurar switch de contingencia
- Contactar a proveedor ISP
- Enrutar el tráfico en switch disponibles
- Configurar el firewall

3.3.10.2. Si es un evento que afectó la infraestructura de servidores.

- Configurar y activar los servidores de contingencia
- Reiniciar los servidores web de emergencia

3.3.10.3. Si es un evento que afectó Infraestructura de Bases de datos, Almacenamiento y Respaldo.

- Recuperación de información y bases de datos desde los respaldos.
- Utilizar los SAN con los datos de contingencia.
- Configurar los servidores de contingencia.

3.3.11. El Líder responsable de la plataforma afectada solicita la contratación urgente de los servicios y equipos necesarios para solucionar el incidente.

3.3.12. El Director de Informática y Desarrollo realiza la gestión para la contratación o compra de los servicios y/o equipos necesarios para solucionar el incidente.

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

3.3.14. El Director de Informática y Desarrollo comunica la solución del incidente a la entidad.

3.3.15. Se define la estrategia de retorno a la normalidad teniendo en cuenta:

- Fecha del retorno y operación normal
- Aplicar el proceso de retorno y mantener la integridad de los datos
- Sincronizar los puestos de computo

3.4. ACTIVIDADES DE MANEJO DE CRISIS

Se listan las actividades y consideraciones necesarias para el manejo de la crisis.

3.4.1. El equipo de Manejo de Crisis evalúa la crisis y el impacto que puede tener para la reputación, imagen u operación de la entidad, al igual que define las acciones para afrontar la crisis.

3.4.2. El equipo de Manejo de Crisis comunicará la crisis a nivel interno y externo, en caso de ser requerido, teniendo en cuenta los siguientes aspectos:

- Información concreta de la crisis
- Proceso en verificación
- Información comprometida
- Afectaciones y alcance

Se tiene en cuenta el informe de la crisis de forma rápida y periódica siendo honestos con la información suministrada emitiendo un reporte de lo más exacto posible.

Se tendrá en cuenta para este informe de crisis la opinión pública, el gobierno, usuarios, contratistas y proveedores.

3.4.3. El equipo de Manejo de Crisis deberá realizar monitoreo permanente de la crisis y tomar las decisiones que correspondan para continuar con la mitigación de este. Se debe tener en cuenta en este manejo lo siguiente:

- Información de los medios
- Información interna
- Impacto sobre la información obtenida

3.5. ACTIVIDADES DE MANTENIMIENTO

Se genera después del incidente la actualización del reporte DRP realizando cambios en la plataforma tecnológica generando resultados de las pruebas y procedimientos que requieren una actualización, apoyándose en auditorias y pruebas actualizadas.

NO	Actividad	Responsable	Frecuencia
1	- Actualizar el DRP, de acuerdo con los Inconvenientes y oportunidades de mejora encontrados. - Velar por la actualización y pruebas de la DRP.	- Líderes de procesos.	- Por cada cambio o contingencia.

2	- Actualizar el DRP, de acuerdo con los Inconvenientes y oportunidades de mejora encontrados. - Sincronizar la configuración de restablecimiento	- Líder de infraestructura	- Permanente
3	- Ejecución de pruebas periódicas verificando el funcionamiento del software.	- Profesionales especializados	- Cada trimestre

3.6. ACTIVIDADES DE PRUEBA

Se debe entregar una copia completa del DRP a los lideres de infraestructura, líderes de procesos e infraestructura, dando una copia completa al sector de redes y comunicaciones.

3.6.1. Recursos mínimos requeridos para el funcionamiento y cumplimiento de la misión de la organización.

3.6.2. Actividades de recuperación y contingencia como las siguientes:

- Configurar switch de contingencia en caso de falla
- Desconectar centro de cableado
- Desconexión de servidores
- Mantenimiento correctivo
- Reinicio de servidores
- Corrección de falla
- Verificar funcionamiento
- Realizar reporte de corrección
- Comunicar reporte a funcionarios