METODOLOGÍA PARA EL DISEÑO DE UN PLAN DE RECUPERACIÓN ANTE DESASTRES O DRP

La metodología recomendada en este documento para el desarrollo de un plan de recuperación ante desastres o DRP para los sistemas de información críticos de TI**,** propone un proceso comprendido desde el inicio del proyecto hasta la realización de las pruebas[1]. Se considera también realizar un análisis de riesgo, estrategias de recuperación y la definición de roles y responsabilidades. La figura 1, presenta las fases de esta metodología, basada en las recomendaciones del NIST, DRII y el BCI, también apoyada en la experiencia de casos prácticos realizados en nuestro país:

1. Inicio del proyecto Plan de Recuperación ante desastres
2. Análisis de impacto sobre el negocio (BIA)
3. Análisis de riesgo
4. Desarrollo estrategias de recuperación para el DRP
5. Roles y responsabilidades
6. Pruebas del DRP

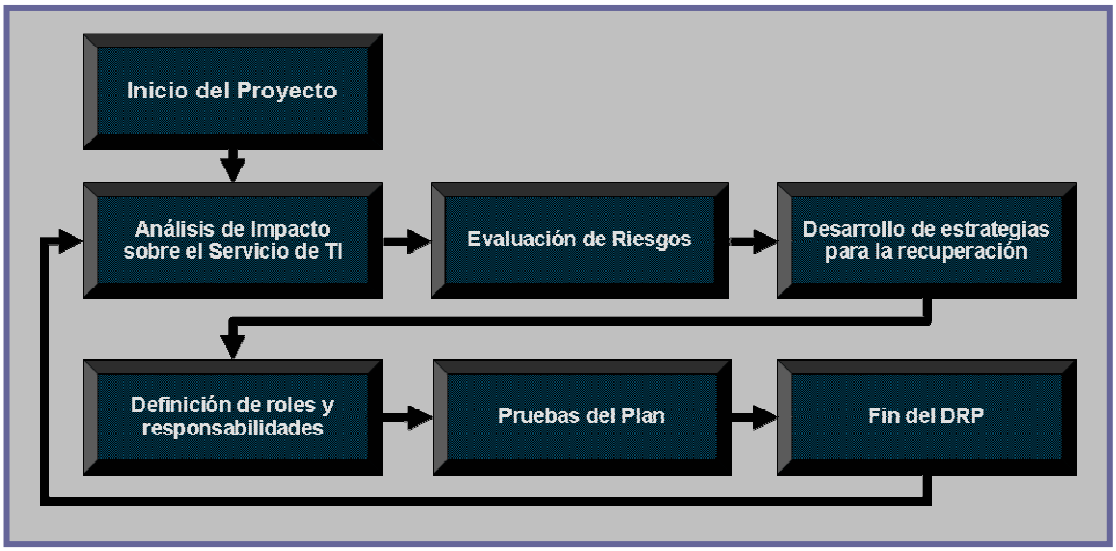

Figura 1. Metodología para un DRP

INICIO DEL PROYECTO

Se realiza en esta fase un conocimiento de la organización. Se evalúa, en esta fase, la documentación existente. Se documentan los beneficios y se deben definir también las personas que tendrán alguna responsabilidad en el proyecto. Otras actividades, de esta fase, se presentan a continuación:

[1] En algunas metodologías se incluye actividades como entrenamiento y mantenimiento del Plan, que no fueron aquí consideradas por razones de prioridad.

1. Revisión de los procesos críticos a considerar en el DRP.
2. Entendimiento de TI
3. Valoración de los riesgos
4. Evaluación del nivel en el que se encuentra la organización y propuestas de acciones a seguir para mejorar los niveles de respuesta ante eventos que afecten la entrega de servicios.

A continuación, se describen cada una de las actividades de esta fase.

1. **Validar el objetivo de continuidad del proyecto**: se establece el objetivo de continuidad (comunicación de crisis, evacuación, respuesta a ciber-incidentes, contingencia, recuperación de desastres y/o continuidad) que tendrá el proyecto DRP y los conceptos que serán utilizados para el mismo.
2. **Acordar el compromiso con las directivas**: se confirma la aprobación de las Directivas de la empresa para la realización del proyecto y la existencia de los recursos financieros, humanos y logísticos requeridos.
3. **Conformar el equipo del DRP**: se asignan responsables para la ejecución del proyecto, identificando al gerente y a las personas que desarrollarán las diferentes actividades.
4. **Refinar el alcance del proyecto**: se revisa y aprueba el alcance del proyecto, para lo cual se considera el objetivo de continuidad establecido, los procesos del servicio que deben incluirse y las dependencias interesadas en el Plan de recuperación ante desastres.

IMPACTO SOBRE EL NEGOCIO (BIA)[2]

El análisis del impacto sobre el negocio (BIA) es uno de los aspectos más importantes a considerar en el desarrollo de un plan de recuperación ante desastres o DRP. Se trata pues, de identificar los diversos eventos que pudieran afectar la continuidad de sistemas críticos de la información.

A continuación la descripción de estas actividades:

1. **Identificar sitios físicos**: se valida la lista de instalaciones físicas o entidades en donde opera los servicio de TI de la empresa.
2. **Identificar sistemas de información**: se obtiene la lista de los sistemas de información que se poseen en cada instalación y se determina cuáles de ellos están relacionados de manera directa o indirecta con el servicio de TI.
3. **Evaluar la criticidad de los sistemas de información**: se califica la criticidad de cada uno de los procesos relacionados con la Empresa, haciendo uso de la tabla de criticidad previamente definida[3].

[2] Business impact analysis

4. **Determinar el RTO, RPO y MTD de cada sistema**: se estima, mediante encuestas o entrevistas, el tiempo de recuperación objetivo, el punto de recuperación objetivo y el tiempo máximo tolerable fuera de servicio para cada proceso en cada instalación con el fin de ayudar en la definición de las estrategias de recuperación.

EVALUACIÓN DE RIESGO Y GESTIÓN DEL RIESGO

La gestión de riesgo es el punto central de la definición de una estrategia de seguridad perfectamente alineada con la visión de las empresas, dentro de su entorno de operación. Esta metodología es el resultado de la combinación de diferentes propuestas existentes en la industria, y utiliza métodos tanto cualitativos, como cuantitativos, los primeros permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los segundos nos permiten la precisión y exactitud, necesarias a la hora de tomar decisiones de tipo financiero, por ejemplo, en el caso de la selección de los controles adecuados, para mitigar un posible evento negativo a la operación y continuidad de los procesos. Para esta actividad nos basamos en AU NZ 4360, COBIT 4.1, ITIL V3, ISO 27005, ISO 13335, ISO 27001, ISO 27002 y COSO.

Identificar amenazas sobre los sistemas

Las entidades a nivel nacional, en Colombia, por ejemplo, enfrentan numerosas amenazas comunes tales como el potencial de falla de un servidor o la pérdida del fluido eléctrico; pero también enfrentan otras amenazas que son especificas para esta entidad o son únicas consideradas desde el punto de vista de su impacto potencial.

Para la identificación de las amenazas a las que pueden enfrentarse los proceso críticos del sistema se deben realizar entrevistas con expertos de la organización, quienes suministrarán información sobre cuáles son las amenazas con mayor impacto, desde la perspectiva de continuidad del servicio y de sus procesos y sistemas críticos, las que podrían llegar a afectar el sistema, es decir, que podrían causar pérdida financiera por demandas, pérdida de imagen por la degradación del servicio.

Identificar vulnerabilidades de los sistemas

Una de las preocupaciones más importantes de los profesionales de la seguridad de la información es el aumento en la cantidad de vulnerabilidades encontradas en los sistemas tecnológicos, las cuales son el blanco predilecto de herramientas de software cada vez más poderosas en su

[3] Ver capítulo Business Impact Análisis – BIA.

capacidad de ocasionar daños a los sistemas de información y la infraestructura que los soporta.

Lo anterior nos lleva a pensar que se necesita contar con una estrategia más coherente y efectiva para mitigar esta inquietante y crítica amenaza, por tanto en el marco del proyecto de implementación del DRP, se le informará a la empresa de las vulnerabilidades de software asociadas a sus sistemas de información y elementos considerados como críticos en la prestación de sus servicios. Se establece, de esta manera, el conjunto de vulnerabilidades que posee cada proceso crítico del servicio de la entidad que al ser explotadas por una amenaza afectarían la operación del sistema.

Cálculo de la probabilidad de ocurrencia de un evento

Nos podemos ayudar para determinar la probabilidad de ocurrencia de ciertos eventos, como el caso de una pérdida de potencia, falla en las comunicaciones, información obtenida de ciertas publicaciones tecnológicas como Information Week e Infosecurity News, CERT, SANS, ASIS, NFPA, EIA e ISO, entre otros, junto con experiencias de casos colombianos.

ESTRATEGIAS DE RECUPERACION Y CONTINUIDAD DEL NEGOCIO

Las estrategias de recuperación están basadas obviamente en los resultados obtenidos luego de la realización del BIA (Business Impact Análisis), en donde también se consideran los valor de los tiempos máximos permitidos de no disponibilidad (MTD). Realizando también un análisis de la toda la información obtenida de las entrevistas, entendimiento de los procesos de negocio, BIA, MTD, procederemos a organizar esta información en una tabla ordenada de prioridades de recuperación de las diferentes sistemas considerados como críticos.

Los elementos a considerar son:

- Sistemas telefónicos
- Redes Locales
- Redes WAN
- Redes MAN
- Internet
- Personas
- Infraestructura física
- Aplicaciones
- Hardware
- Bases de datos
- Sistemas operativos

- Firewalls
- IDS-IPS
- Switches
- Routers

Las estrategias a seguir se describen a continuación:

1. Hot sites: Normalmente esta configurado con todo el hardware y el software requerido para iniciar la recuperación a la mayor brevedad.
2. Warm sites: En esta opción no se incluyen servidores específicos de alta capacidad.
3. Cold sites: En esta opción sólo se tiene aire acondicionado, potencia, enlaces de telecomunicaciones, y otros.
4. Sitios móviles
5. Acuerdos recíprocos con otras organizaciones
6. Mirror site: Se procesa cada transacción en paralelo con el sitio principal.
7. Múltiples centros de procesamiento

Sitio	Costo	Hardware	Telecomuni-caciones	Tiempo	Localización
Sitio en frío	Bajo	No	Ninguno	Largo	Fijo
Sitio semi-preparado	Medio	Parcial	Parcial	Medio	Fijo
Sitio preparado (hot site)	Alto	Completo	Parcial	Corto	Fijo
Sitio Móvil	Alto	Variable	Variable	Variable	No fijo
Espejo (Mirror)	Muy Alto	Completo	Completo	Mínimo	Fijo
Sitio Reciproco	Bajo	Parcial	Parcial	Medio	Fijo

Figura 2. Estrategias utilizables para la recuperación

ROLES Y RESPONSABILIDADES

Para cada una de las estrategias de mitigación y reducción establecidas. deben identificarse los métodos, plazos, personas, recursos y tareas necesarias para implementarlas. Igualmente, deben establecerse las estructuras organizacionales, los perfiles de los cargos y los procesos, que darán sostenibilidad a la continuidad del servicio de TI (ver figura 3). La definición de roles y responsabilidades es uno de los aspectos más importantes del Plan de Recuperación ante desastres, porque aquí se determinan cada una de las actividades de los responsables de ejecutar el Plan, y estas actividades corresponden a las que hay que ejecutar antes, durante y después del desastre.

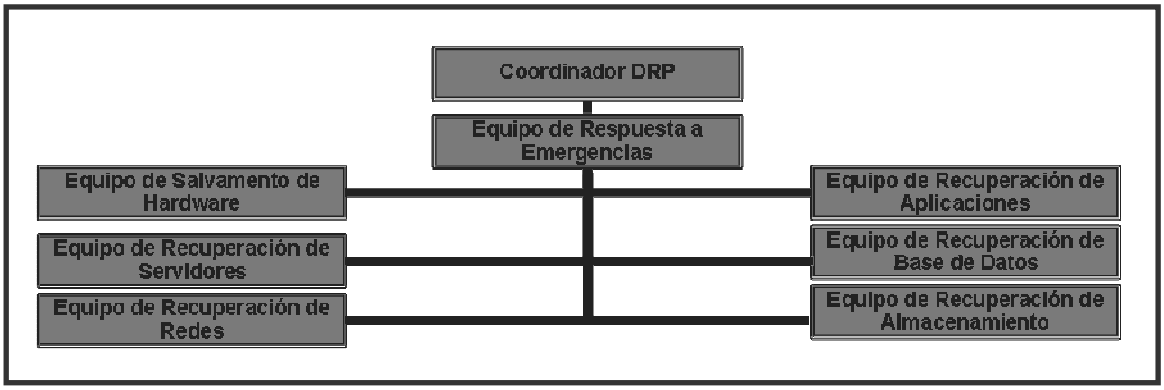

Figura 3. Roles y responsabilidades para desarrollar un DRP.

PRUEBAS DEL PLAN

La efectividad del DRP en situaciones de emergencia se puede valorar si existe un plan de prueba que se lleve a cabo en condiciones reales. La fase de prueba debe contener las actividades más importantes que requieran comprobación y certeza en su funcionamiento futuro.

Se debe probar dentro de un ambiente que simule las condiciones que serían aplicables en una emergencia verdadera. Es también importante que las pruebas se lleven a cabo por las personas que serían responsables de esas actividades en una crisis. Estas pruebas comprenden:

1. Desarrollo de los objetivos y alcance de la prueba
2. Configuración del ambiente de prueba
3. Preparación de los datos de la prueba
4. Identificación de quién dirigirá la prueba
5. Identificación de quién controla y supervisa la prueba
6. Preparación de cuestionarios de evaluación
7. Preparación de presupuesto para la fase de prueba
8. Entrenamiento a los grupos de prueba de las unidades de negocio

Autor: Rodrigo Ferrer
Ing Eléctrico, con especialización en Telemática y Gerencia de Sistemas de información, Magíster en filosofía y es CISSP, CISA, ABCP, CSSA, CST y COBIT 4.1 Foundation Certificate.
rodrigo.ferrer@sisteseg.com
Bogotá
Colombia.