



NEWITS

Servizi per le nuove tecnologie dell'informazione

Disaster Recovery Planning

Esempio di approccio metodologico al problema

13 Maggio 2008

Esempio NEWITS

Indice

INDICE.....	2
INFORMAZIONI GENERALI.....	3
CONTROLLO DI VERSIONE	3
DEFINIZIONI E REQUISITI	4
<i>Generalità.....</i>	4
<i>Obiettivi generici di progetto</i>	4
<i>Livelli di servizio del Disaster Recovery</i>	5
MODALITÀ DI IMPLEMENTAZIONE	7
<i>Generalità.....</i>	7
<i>Fase 1 - Attività propedeutiche al progetto (Project Initiation).....</i>	7
<i>Fase 2 – Analisi degli assets.....</i>	7
<i>Fase 3 - Analisi degli impatti (Business Impact Assessment).....</i>	8
<i>Fase 4 - Definizione dettagliata dei requisiti e della fattibilità.....</i>	8
<i>Fase 5 – Sviluppo del piano di Disaster Recovery.....</i>	9
<i>Fase 6 – Sviluppo del piano di test/verifica.....</i>	9
<i>Fase 7 – Sviluppo del piano di manutenzione del sistema.....</i>	9
<i>Fase 8 – Implementazione iniziale e collaudo</i>	10
INDICE DEL PIANO DI DISASTER RECOVERY	10

Proprietà

Le informazioni contenute nel presente documento sono di proprietà della Newits s.a.s. di C.Aiolfi & C. Per nessun motivo questo documento o parte di esso può essere riprodotta in qualsiasi forma o mezzo (inclusa la registrazione e la fotocopia) senza autorizzazione scritta da parte della Newits s.a.s. di C.Aiolfi & C.

Informazioni Generali

Controllo di versione

Versione	Data	Autore	Sommario modifiche
1.0	13/5/2008	C.Aiolfi	Versione originale

Esempio NEWITS

Definizioni e requisiti

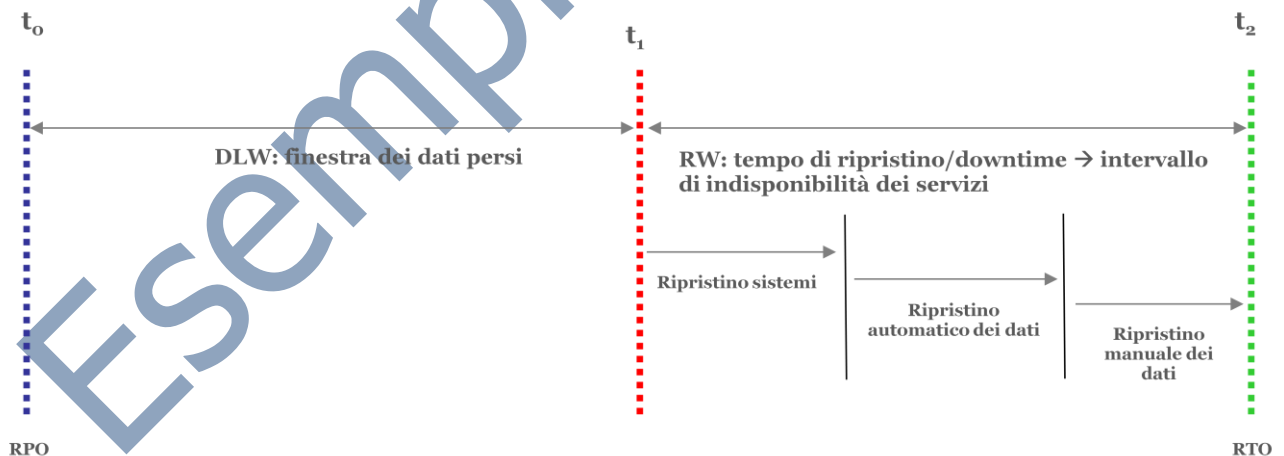
Generalità

Nella realtà quotidiana, tutte le organizzazioni e perfino l'utente di casa dovrebbero predisporre un proprio piano di ripristino in caso di disastro. E' fin troppo ovvio che tale piano sarà commisurato alle caratteristiche stesse dell'azienda (dimensioni, tipo di attività, rilevanza sul mercato, criticità delle informazioni trattate e altri fattori che verranno analizzati successivamente). Tuttavia qualche precisazione è necessaria. I termini "Business Continuity" e "Disaster Recovery" fanno parte del "dominio dell'emergenza" e sono spesso erroneamente usati come sinonimi. La "Business Continuity" ha come obiettivo quello di evitare l'interruzione del business in generale e prende quindi in considerazione tutti i servizi ed i processi aziendali. Il Disaster Recovery invece tiene conto solo di eventi disastrosi, che si possono definire "estremi" (quegli eventi cioè a scarsa probabilità di accadimento, ma ad alto impatto sul business) e che sono in grado di provocare un danno di rilevante entità sulla continuità operativa dei servizi IT. In poche parole il Disaster Recovery si colloca all'interno della Business Continuity e considera solo l'IT ovvero l'insieme del sistema informatico e di tutte le risorse ad esso relative (le persone che lo gestiscono, l'organizzazione, le politiche e le procedure correlate, i siti ove è collocato).

Si potrebbe quasi dire che obiettivo ultimo di un progetto di Business Continuity sia la definizione di un Disaster Recovery, che dunque rappresenta l'insieme di quegli adempimenti di tipo fisico, logico, organizzativo, amministrativo, logistico e legale, atti a fronteggiare un evento a carattere catastrofico, che renda indisponibili le risorse deputate alle operazioni di elaborazione dei dati. Il Disaster Recovery è in sostanza un "processo" che consente di ripristinare il normale o indispensabile funzionamento dell'operatività aziendale e il trattamento dei dati precedentemente interrotti da un evento indesiderato di natura eccezionale e cioè da quello che può definirsi quale vero e proprio "disastro" in un sistema informatico automatizzato.

Obiettivi generici di progetto

I progetti per l'implementazione di un processo di Disaster Recovery sono spesso caratterizzati dalla loro capacità di raggiungere tre obiettivi: il punto di ripristino, il tempo di ripristino ed il budget. La figura seguente può aiutare ad illustrare questi concetti.



- T_1 rappresenta l'ora dell'evento disastroso.
- T_0 è il tempo al quale i dati salvati possono ritenersi certamente validi. T_0 è il punto di ripristino e rappresenta lo stato in cui i dati regrediscono dopo il ripristino (es. ripristino dall'ultimo backup). L'intervallo DLW (Data Loss Window) tra T_0 e T_1 identifica il periodo in cui i dati prodotti dal sistema informativo non sono recuperabili ovvero la quantità di dati persi. (es. intervallo di tempo tra il momento dell'evento disastroso e l'ultimo backup valido usabile per il ripristino).

- T_2 è l'ora di completo ripristino dei dati. T_2 rappresenta il momento in cui i dati vengono ripristinati nello stato in cui si trovavano al momento del disastro T_1 (es. ripristino dall'ultimo backup + caricamento manuale)
- RW (Recovery Windows) è il tempo necessario per il pieno ripristino del sistema informativo.
- RPO (Recovery Point Objective) corrisponde alla dimensione della finestra di tempo DLW e rappresenta l'obiettivo del progetto di recovery. Minore il valore e migliore è il risultato.
- RTO (Recovery Time Objective) coincide con il tempo di fermo dei sistemi e quindi di indisponibilità dei servizi applicativi. E' uno degli obiettivi di progetto; minore il valore e migliore è il risultato..

Livelli di servizio del Disaster Recovery

Le soluzioni di DR sono spesso descritte in termini di livello di servizio. Questi livelli di servizio furono inizialmente introdotti nel 1993 dal Technical Steering Committee di SHARE (www.share.org) e variano dal livello 0, che non prevede alcuna soluzione di DR, al livello 6 che implementa una soluzione integrata hardware e software per raggiungere l'obiettivo "zero perdita dati" e ripartenza immediata.

Service Tier 0: No Off-Site Storage of Data

Service Tier 0 is the lack of a DR solution. Nearly all facilities using this approach back up their data but store the backups on site, unlike the other six true DR solutions, in which backups are stored off site. If a catastrophic event occurs, such facilities may be able to restore their data from backup—as long as the damage caused by the data does not also prevent access to the backups. Large natural disasters or intentional acts of destruction are usually not so selective in their effects, however. It is much more likely that an entire building or even several city blocks or more are affected; few large-scale disasters target a single floor of a building and leave the others undamaged.

Service Tier 1: Pickup Truck Access Method

The Pickup Truck Access Method (PTAM) is not, strictly speaking, a DR solution. It is a commonly used practice for protecting data that has been applied to the problem of DR. PTAM consists of backing up data, most often to tape, although any easily transportable storage media will do, and then physically transporting the backup media to a different location for storage. When the data is needed, it is transported to a cold site, which has the infra structure necessary to support servers, storage, and networks, and only then is the hardware purchased and installed. One advantage of this solution is its relative low cost—if no disaster occurs. The down side, however, is that if disaster strikes, establishing a new data center at the cold site will take considerable time, money, and labor. Another disadvantage is the impracticality of testing this solution.

Service Tier 2: PTAM Plus Hot Site

Like Service Tier 1, the Service Tier 2 solution consists of backing up data to portable storage media and then physically transporting the media to an alternate location. The difference is that when the data is needed, it is transported to a hot site, where the hardware is already up and running. Advantages over the previous solution include a much shorter recovery time and the ability to test the method before a data happens. In addition, compared to the solutions represented by the higher service tiers, the Service Tier 2 solution is still relatively low cost.

Service Tier 3: Electronic Vaulting

Like Service Tiers 1 and 2, the first part of this method consists of backing up the data. Unlike the previous solutions, however, in which the media containing the backup data is transported

physically, electronic vaulting transports the data electronically to the hot site. This reduces the amount of time needed to transport the data, resulting in faster recovery time. Savings in physical transportation costs are also achieved. These savings, however, are more than offset by the cost of the telecommunication.

Service Tier	Storage Media		Solution				Data Loss Window		Downtime	
	Type Often Used	Reliability	Cost	Ease of Use	Labor Required (Recover)	Testability	RPO	Completeness	RTO	Availability
Tier 1	Tape	Poor	Low	High	High	None	Day+	Poor	Week+	Poor
Tier 2	Tape	Poor	Low to moderate	High	High	Moderate	Day+	Poor to good	Day+	Poor
Tier 3	Tape	Poor	Moderate	High	High	Moderate	< Day	Poor to good	< Day	Poor to moderate

Service Tier 4: Two Active Sites

A Service Tier 4 solution can address the disadvantages of solutions from Service Tiers 1 through 3. A Service Tier 4 solution consists of two active sites, where each acts as a backup site to the other. One requirement for this solution is that the sites should be at some distance from each other to ensure that the same data will not put both of them out of commission. In addition, each site must have enough unused processing capacity that it can absorb the other site's workload if need be. This solution has two variations. The first variation is similar to electronic vaulting, in that data is backed up and transmitted electronically from each site to the other. The major difference between the Service Tier 3 and Service Tier 4 solutions is whether the second site is active or idle. The second variation replicates data, either through continuous transmission of data or through dual online storage. The use of replication in the second variation significantly shrinks the size of the data-loss window, and consequently improves the completeness of the recovery. With an automatic network-switching capability, a Service Tier 4 solution can reduce data recovery to hours or even minutes.

Service Tier 5: Two Active Sites with Two-Phase Commit

As with Service Tier 4, the Service Tier 5 solution consists of two active sites, each with enough unse processing capacity that it can take on the other's workload if data strikes. The difference is that, for selected data, when an application initiates a request to update the data, the application is not notified that the update is complete until both sites have concluded the update operation. Facilities using this solution can only lose data that is in the process of being updated. One disadvantage of this solution is that it increases the time required to update data, since the application has to wait for the update request and acknowledgement to be transmitted to the remote site.

Service Tier 6: Zero Data Loss

As with the Service Tier 4 and 5 solutions, a Service Tier 6 solution consists of two active sites, each with enough unused processing capacity that it can take on the other's workload in the event of a data. The difference is that a Service Tier 6 solution immediately and automatically transfers one site's workload to the second site when a data occurs. This solution requires dual online storage and an automatic network-switching capability. One disadvantage of this solution is that its high cost quite often leads to increased complexity. The reason for this is that if an organization implements a Service Tier 6 solution, the organization will usually only use that solution for its business-critical data. Less costly solutions from lower service tiers will be employed for less critical data. Using solutions from several different service tiers, however, increases the complexity in planning and implementing data recovery.

Service Tier	Storage Media	Solution	Data Loss Window	Downtime
--------------	---------------	----------	------------------	----------

	Type Often Used	Reliability	Cost	Ease of Use	Labor Required (Recover)	Testability	RPO	Completeness	RTO	Availability
Tier 4	FC drives	Very high	High	Low	Moderate to low	Good	Seconds	Moderate to good	Minutes	Moderate to good
Tier 5	FC drives	Very high	High	Low	Low	Good	Seconds	Good	Seconds	Good
Tier 6	FC drives	Very high	Very high	Low	Very low	Excellent	None	Excellent	Seconds	Excellent

Modalità di implementazione

Generalità

Lo studio proposto è finalizzato a definire gli aspetti tecnici (rilevazione dell'architettura attuale del sistema informativo e definizione di alcune alternative tecnologiche per l'implementazione del DR), strategici (obiettivi e budget), organizzativi (definizione di ruoli e procedure, formazione del personale), economici (analisi dei costi) e, non ultimi, quelli legali (leggi, regolamenti, codici di condotta, raccomandazioni) di un piano di Disaster Recovery.

La metodologia generale di progetto proposta consiste di otto fasi separate; la metodologia è conforme alle direttive del DLGs 196/2003.

Fase 1 - Attività propedeutiche al progetto (Project Initiation).

Questa fase è usata per ottenere un conoscenza base dell'ambiente IT corrente e dei piani di sviluppo. Vengono definiti:

- Rifinitura degli obiettivi di progetto
- Definizione dettagliata delle attività
- Definizione del gruppo di lavoro
- Pianificazione delle attività
- Analisi preliminare dei rischi di progetto

Metodo: Incontri presso la sede del cliente, documentazione

Deliverables: DRPDR101 Obiettivi ed introduzione

Fase 2 - Analisi degli assets.

In questa fase debbono essere considerati e attentamente valutati gli "asset", ossia le componenti base del sistema informativo aziendale.

Occorre anzitutto stabilire (in ordine di priorità) quali elementi hardware e quali applicazioni software (incluse le banche-dati) siano indispensabili per l'attuazione dei processi automatizzati di trattamento dei dati. La classificazione delle applicazioni viene fatta in base a fattori che ne determinano il rispettivo peso. Tali fattori sono i seguenti: livello di criticità attribuito alle applicazioni, valutazione qualitativa e tempo massimo di indisponibilità delle stesse.

Sul piano della valutazione qualitativa, occorre effettuare una stima della possibile o probabile perdita economica dovuta al mancato utilizzo di ognuna delle applicazioni. Siffatta stima può essere rappresentata attraverso diversi livelli di danno

E' infine necessario stabilire il tempo massimo di indisponibilità e di inoperatività delle applicazioni sopportabile dall'azienda per non perdere la sua posizione sul mercato e la sua credibilità (vedi RTO).

Tuttavia l'analisi degli asset non può esaurirsi con le valutazioni pertinenti alle applicazioni. È necessario classificare anche gli elementi idonei al corretto ripristino. E ovviamente non si può prescindere né dall'esistenza di un sito alternativo ove ricoverare le infrastrutture prima che sia

riattivato il sito principale né dalla analisi delle procedure di "backup" e dei relativi metodi di archiviazione.

Metodo: Workshop, raccolta documentazione esistenze, documentazione

Deliverables: DRPDR102 Architettura di sistema

Fase 3 - Analisi degli impatti (Business Impact Assessment).

In tale fase vengono evidenziati i principali rischi conseguenti a calamità naturali o ad altri eventi imprevedibili di rilevante entità, che possono avere impatti estremi sulla funzionalità dell'infrastruttura I.T. e quindi sul funzionamento del business in generale. È chiaro quindi che il piano di DR deve prendere in considerazione solo alcuni tipi di minacce (quelle relative al dominio dell'emergenza), come è altrettanto ovvio che, per quel che concerne i dati personali (sensibili e giudiziari), l'analisi dei rischi fatta in tale sede si colloca all'interno della più generale analisi dei rischi prevista parte integrante del contenuto del D.P.S richiesto dal DLGs 196/2003.

Analizzate le tipologie di rischi che interessano il piano di DR si passa a svolgere una dettagliata analisi sull'impatto che tali rischi possono avere sull'azienda. Tramite tale analisi si considerano le conseguenze del disastro in relazione a determinate variabili, rappresentate dal tempo massimo di ripartenza (strettamente collegato al tempo massimo di indisponibilità delle applicazioni, come si è visto in precedenza) e dalla definizione delle priorità di ripristino (e cioè dall'individuazione dei dati e dei sistemi, che vanno ripristinati con precedenza assoluta sugli altri). Riguardo ai dati personali, la legge fissa il tempo massimo di ripristino in sette, ma naturalmente i tempi dipendono dal tipo di dati trattati e dai diritti oggetto di tutela.

A questo punto si può stabilire quale sia la massima perdita tollerabile di dati e cioè quale sia il massimo rischio sostenibile, in relazione ad una certa scala di valori.

Metodo: Workshop, raccolta documentazione esistenze, documentazione

Deliverables: DRPDR103 Inventario dei sistemi critici

Fase 4 - Definizione dettagliata dei requisiti e della fattibilità

I fattori da considerare ai fini della scelta della soluzione di DR più aderente alle esigenze dell'organizzazione sono molteplici. Anzitutto va tenuta in conto la situazione iniziale dell'infrastruttura con tutti i suoi asset; è necessario poi verificare i risultati sia dell'analisi dei rischi attinenti al dominio dell'emergenza sia della B.I.A.; infine c'è da valutare l'infrastruttura per il recovery (ubicazione, struttura del datacenter alternativo, risorse di rete, back-up, personale, elementi di supporto). Il tutto è finalizzato a rispondere ai seguenti quesiti fondamentali:

- se la soluzione di DR prescelta sia funzionale al ripristino;
- se consenta un ripristino solo parziale o totale (RPO);
- in quanto tempo si ottenga il ripristino e inoltre come, dove, quando e ad opera di chi (RTO);
- quanti e quali soggetti e infrastrutture debba interessare.

A questo punto è necessaria l'analisi dei costi (analisi di tipo quantitativo, che si affianca alla precedente valutazione qualitativa dei danni effettuata nella fase di analisi degli asset, poiché la scelta dell'una o dell'altra soluzione di DR potrà essere più o meno economica: maggior sicurezza è sinonimo di costi alti, viceversa a costi bassi si otterrà un livello di sicurezza minore.

Occorrerà trovare un giusto equilibrio tra i costi di infrastruttura per il D.R. ("soportabile livello di spesa") e le perdite economiche dovute all'evento disastroso ("ragionevole controllo del rischio"). Quest'ultima variabile è molto importante in quanto in essa rientrano non soltanto le perdite patrimoniali e quelle di dati critici, ma anche i costi pertinenti alla gestione del periodo post-crisi e al rischio di una pubblicità negativa per l'azienda, soprattutto nei casi in cui il disastro sia stato causato da attività umana. Per altro vanno valutati gli obblighi e le responsabilità in caso di propagazione dei danni ad un'altra organizzazione.

Metodo: Workshop, raccolta documentazione esistenze, documentazione

Deliverables: DRPDR104 Principi di base

Fase 5 – Sviluppo del piano di Disaster Recovery

La fase di progettazione del DR si articola essenzialmente in due sottofasi: un piano generale o di massima ed un piano di dettaglio.

Il piano generale deve, in primo luogo, descrivere l'architettura complessiva da realizzare (aspetti logistici), comprensiva delle componenti hardware e software. Si devono cioè individuare, oltre al sito del datacenter alternativo, i luoghi ove collocare fisicamente i singoli elementi di ripristino. In secondo luogo occorre fissare gli obiettivi da perseguire (aspetti strategici), in relazione alle priorità stabilite nelle precedenti analisi degli asset, dei rischi e del corrispondente impatto sui dati, sui sistemi e sui beni patrimoniali. Infine bisognerà rispettare i vincoli economici (rispetto del budget stanziato dai vertici aziendali per la realizzazione del piano) e legali (v. le prescrizioni del DLGs 196/2003 e dell'All.B per il trattamento di dati personali e v. altre normative menzionate in precedenza).

Al piano di massima segue il piano di dettaglio sviluppato secondo le usuali "best practice" di gestione dei progetti informatici; in generale il piano si sviluppa in tre momenti:

- a) Progettazione.
 - a. Analisi di dettaglio delle componenti hardware e software, gap analysis
 - b. Definizione delle procedure di gestione del sistema con definizione di ruoli, funzioni e responsabilità (chi-deve-fare-cosa).
 - c. Definizione delle fasi di gestione dell'emergenza:
 - i. fase di contenimento
 - ii. attivazione del livello minimo di operatività da DR site
 - iii. attivazione del livello massimo di operatività da DR site
 - iv. valutazione dei danni
 - v. riacquisto dei beni danneggiati
 - vi. ripristino del site di produzione
 - vii. riattivazione dei servizi sul site di produzione
- b) Pianificazione delle attività. Vengono qui indicate le attività e il tempo necessari alla realizzazione del progetto, i gruppi di lavoro, le conoscenze richieste per ogni singola attività, le modalità di coinvolgimento del personale

Metodo: Workshop, documentazione piano

Deliverables: Sezione 2-3-4-5 del piano di DR (vedi allegato), DPRDR105 Gap Analysis

Fase 6 – Sviluppo del piano di test/verifica

I test in questione sono quelli relativi alla progettazione del piano, non alla simulazione del disastro. Verranno definiti test da effettuarsi periodicamente per verificare la funzionalità dei vari elementi di ripristino, delle applicazioni e delle singole unità operative, in modo da valutare l'efficienza dell'intera infrastruttura. Di siffatte verifiche si dovranno stendere precisi rapporti, secondo modalità prestabilite. Pianificazione della fase di collaudo.

Metodo: Workshop, documentazione

Deliverables: Sezione 6 del piano di DR (vedi allegato)

Fase 7 – Sviluppo del piano di manutenzione del sistema

In questa fase devono essere definite le procedure per la gestione dei cambiamenti e delle revisioni del progetto. Gli aggiornamenti sono infatti necessari e, con riguardo ai dati personali, l'art. 31 del Cod. (disposizione questa estensibile a tutti gli altri dati rilevanti per l'organizzazione) pone l'obbligo di custodire e controllare i dati "anche in relazione alle conoscenze acquisite in base al progresso tecnico". In tal modo, alla natura dei dati e alla tipologia dei trattamenti si aggiunge un altro elemento che permette di determinare quali siano le misure di sicurezza più adatte a ridurre al minimo il rischio di perdita dei dati per qualsivoglia causa ("anche accidentale").

Il piano di gestione dei cambiamenti deve tener conto sia delle variazioni tecnologiche apportate al sistema di produzione che delle mutate esigenze aziendali ed allineare di conseguenza le conoscenze del personale con opportuni piani di formazione.

Metodo: Workshop, documentazione

Deliverables: Sezione 7 del piano di DR (vedi allegato)

Fase 8 - Implementazione iniziale e collaudo

E' la fase del piano che prevede la realizzazione delle componenti infrastrutturali (siti di backup, tecnologie di replica, ridondanza delle infrastrutture di rete, ..), organizzative (DR team) e gestionali (procedure di allineamento, monitoraggio, ...) direttamente legate al DR e non ancora implementate nel sistema informativo aziendale. La fase di implementazione è seguita dalla fase di collaudo.

Metodo: Installazione e test, documentazione

Deliverables: Sezione 6 del piano di DR (vedi allegato)

Indice del piano di Disaster Recovery

Il piano di Disaster Recovery include le informazioni necessarie alla migrazione dei servizi applicativi dal sito primario a quello secondario in caso di sinistro. La struttura del documento è la seguente.

Sezione 1: Informazioni generali sul piano

- DRPDR101: Obiettivi ed introduzione
- DRPDR102: Architettura di sistema
- DRPDR103: Inventario dei sistemi critici
- DRPDR104: Principi di base
- DRPDR105: Gap analysis (infrastruttura, applicazione e procedure)

Sezione 2: Operatività normale

- DRPDR201: Inizializzazione infrastruttura
- DRPDR202: Inizializzazione banche dati
- DRPDR203: Inizializzazione applicazioni
- DRPDR204: Sincronizzazione siti
- DRPDR205: Monitoraggio siti
- DRPDR206: Piano di training del personale
- DRPDR207: Simulazione periodica di ripristino

- DRPDR208: Documentazione delle attività svolte (reporting)

Sezione 3: Lancio della procedura di emergenza

- DRPDR301: Criteri di sicurezza
- DRPDR302: Comunicazioni (Lista dei contatti in caso di disastro, modalità di contatto)
- DRPDR303: Disaster recovery team (ruoli e responsabilità)
- DRPDR304: Attivazione del piano di disaster recovery
- DRPDR306: Valutazione dei danni
- DRPDR307: Procedure di acquisto in emergenza
- DRPDR308: Documentazione delle attività svolte (reporting)

Sezione 4: Lancio delle procedure di avviamento del sito secondario

- DRPDR401: Preparazione del sito di disaster recovery
- DRPDR402: Procedura di ripristino dell'infrastruttura
- DRPDR403: Procedura di ripristino della banche dati
- DRPDR404: Procedura di ripristino delle applicazioni
- DRPDR405: Procedura di ripristino delle operazioni

Sezione 5: Ripristino del sito di produzione

- DRPDR500: Condizioni per il ritorno al sito di produzione
- DRPDR501: Ripristino dell'infrastruttura
- DRPDR502: Ripristino della banche dati
- DRPDR503: Ripristino delle applicazioni
- DRPDR503: Ripristino delle operazioni

Sezione 6: Verifica/test del piano

- DRPDR601: Obiettivi e strategie di test
- DRPDR602: Procedure di test e verifica

Sezione 7: Manutenzione del piano

- DRPDR701: Aggiornamento del piano
- DRPDR702: Lista di riferimento dei documenti di piano