CODAU

Convegno permanente
dei Direttori Amministrativi
e Dirigenti delle Università Italiane

Gruppo di Lavoro ICT - 10 febbraio 2012
Art. 50 bis, continuità operativa, disaster recovery

Agenda dell'incontro

A. Premesse:

    1. Introduzione e sintesi del quadro normativo

    2. Stato di avanzamento dei lavori: sintesi degli incontri avuti con DigitPA, Tavolo Tecnico ICT4University e CINECA in relazione al tema della CO/DR.

B. Individuazione di un approccio comune / linee guida

    1. Definizione del perimetro di analisi ed impatto organizzativo delle scelte

    2. Proposta di articolazione dei servizi oggetto dell'autovalutazione

    3. Proposta di template dello Studio di Fattibilità Tecnica

C. Passi successivi: Piano di Continuità Operativa, Piano di Disaster Recovery, revisioni periodiche

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA Roma - Lunedì, 10 gennaio 2011 SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DECRETO LEGISLATIVO 30 dicembre 2010, n. **235.**

Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.

Continuità operativa e disaster recovery

Art. 50-bis. Continuità operativa.

1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono :

a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

b) il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione. DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA.

Codice dell'Amministrazione Digitale: scadenze

- **Entro 3 mesi** le pubbliche amministrazioni utilizzeranno la posta elettronica certificata o altre soluzioni tecnologiche per tutte le comunicazioni che richiedono una ricevuta di consegna ai soggetti che hanno preventivamente dichiarato il proprio indirizzo
- **Entro 4 mesi** le amministrazioni individueranno un unico ufficio responsabile dell'attività ICT;
- **Entro 6 mesi**
  - Le PA centrali pubblicheranno sui propri siti istituzionali i bandi di concorso e tutta una serie di informazioni sul proprio funzionamento nell'ottica della total disclosure
  - Le amministrazioni consentiranno ovunque i pagamenti ad esse spettanti per via telematica
  - Le amministrazioni e le imprese comunicheranno tra loro esclusivamente per via telematica

Codice dell'Amministrazione Digitale: scadenze

- **Entro 12 mesi**
  - Saranno emanate le regole tecniche che consentiranno di dare piena validità alle firme elettroniche diverse da quella digitale, nonché alle copie cartacee e, soprattutto, a quelle digitali dei documenti informatici, dando così piena effettività al processo di dematerializzazione dei documenti della PA
  - Saranno emanate le regole tecniche per la conservazione sostitutiva dei documenti in forma digitale dando il via agli archivi informatizzati
  - Le pubbliche amministrazioni non potranno richiedere l'uso di moduli e formulari che non siano stati pubblicati sui propri siti istituzionali
  - Il cittadino fornirà una sola volta i propri dati alla pubblica amministrazione. Sarà onere delle amministrazioni (in possesso dei dati) assicurare, tramite convenzioni, l'accessibilità delle informazioni alle altre amministrazioni richiedenti
  - Saranno definite le basi di dati di interesse nazionale
  - Saranno emanate tutte le regole tecniche previste dal CAD
  - Le regole del nuovo CAD si applicheranno, mediante un apposito DPCM, anche alla Presidenza del Consiglio dei Ministri e all'Amministrazione finanziaria
- **Entro 15 mesi** le pubbliche amministrazioni predisporranno appositi piani di emergenza idonei ad assicurare, in caso di eventi disastrosi, la continuità delle operazioni indispensabili a fornire servizi e il ritorno alla normale operatività.

Continuità operativa e disaster recovery: news…

28-11-2011 Emanate le “Linee guida per il disaster recovery delle pubbliche amministrazioni” → http://www.digitpa.gov.it/notizie/emanate-le-linee-guida-disaster-recovery-delle-pubbliche-amministrazioni

05-01-2012 Pubblicata in Gazzetta Ufficiale la Circolare DigitPA sulla Continuità Operativa → http://www.digitpa.gov.it/notizie/continuit-operativa-pubblicata-gazzetta-ufficiale-circolare-digitpa

13-01-2012 Pubblicata la tabella di corrispondenza servizi SPC-soluzioni di DR → http://www.digitpa.gov.it/notizie/pubblicata-tabella-corrispondenza-servizi-spc-soluzioni-dr

Circolare 58

- La **prima parte della Circolare** riporta le informazioni che le Amministrazioni devono inviare a DigitPA ai fini del rilascio del parere sugli Studi di Fattibilità' Tecnica (SFT) e le modalità di presentazione delle richieste come previsto dal comma 4, art. 50 bis del CAD → **FASE 1 o iniziale**
- La **seconda parte della Circolare** riporta le informazioni che le Amministrazioni devono inviare a DigitPA ai fini dell'attività' di definizione ed aggiornamento dei Piani di Disaster Recovery (DR) → **FASE 2 o implementativa**
- Le Amministrazioni, **una volta ricevuto il parere di DigitPA** e definito il Piano di DR devono inviare il predetto Piano a DigitPA per il tramite del **"Responsabile della Continuità Operativa" dell'Amministrazione**
- Con **cadenza annuale, entro il 31 dicembre di ogni anno**, le Amministrazioni devono inviare a DigitPA, da parte del "Responsabile della Continuità Operativa" dalla casella PEC della Amministrazione, la **versione aggiornata del Piano di DR** specificando le **modifiche intervenute** e le **motivazioni** di tali modifiche

Workflow previsto /1

Fase di emissione delle LG

* Emissione delle linee guida di DigitPA;
* Parere del Garante della Privacy;

DigitPA: Emette le Linee Guida (LG) per il DR delle PPAA, sentito il Garante della Privacy.

Fase di avvio e studio delle soluzioni

* Studio della soluzione, stesura studi di fattibilità tecnica secondo il percorso delle LG e richiesta del parere a DigitPA;

PP.AA. : Predispongono e sottopongono al parere di DigitPA Studi di fattibilità tecnica (SFT), tenuto conto dello strumento e delle LG.

DigitPA: emette pareri su SFT.

Fase di realizzazione, gestione e test delle soluzioni

- Realizzazione delle soluzioni di CO e DR; stesura dei piani di CO e DR;
- Verifica – da parte delle PP.AA: - con cadenza biennale del piano di CO;
- Costante aggiornamento dei piani di DR;

PP.AA.:
- implementano le soluzioni e predispongono i piani di CO e di DR sulla base dello SFT e del parere di DigitPA;
- verificano con cadenza biennale la funzionalità del Piano di CO;
- garantiscono la manutenzione della soluzione (aggiornamento dei piani; test periodici) informando DigitPA.

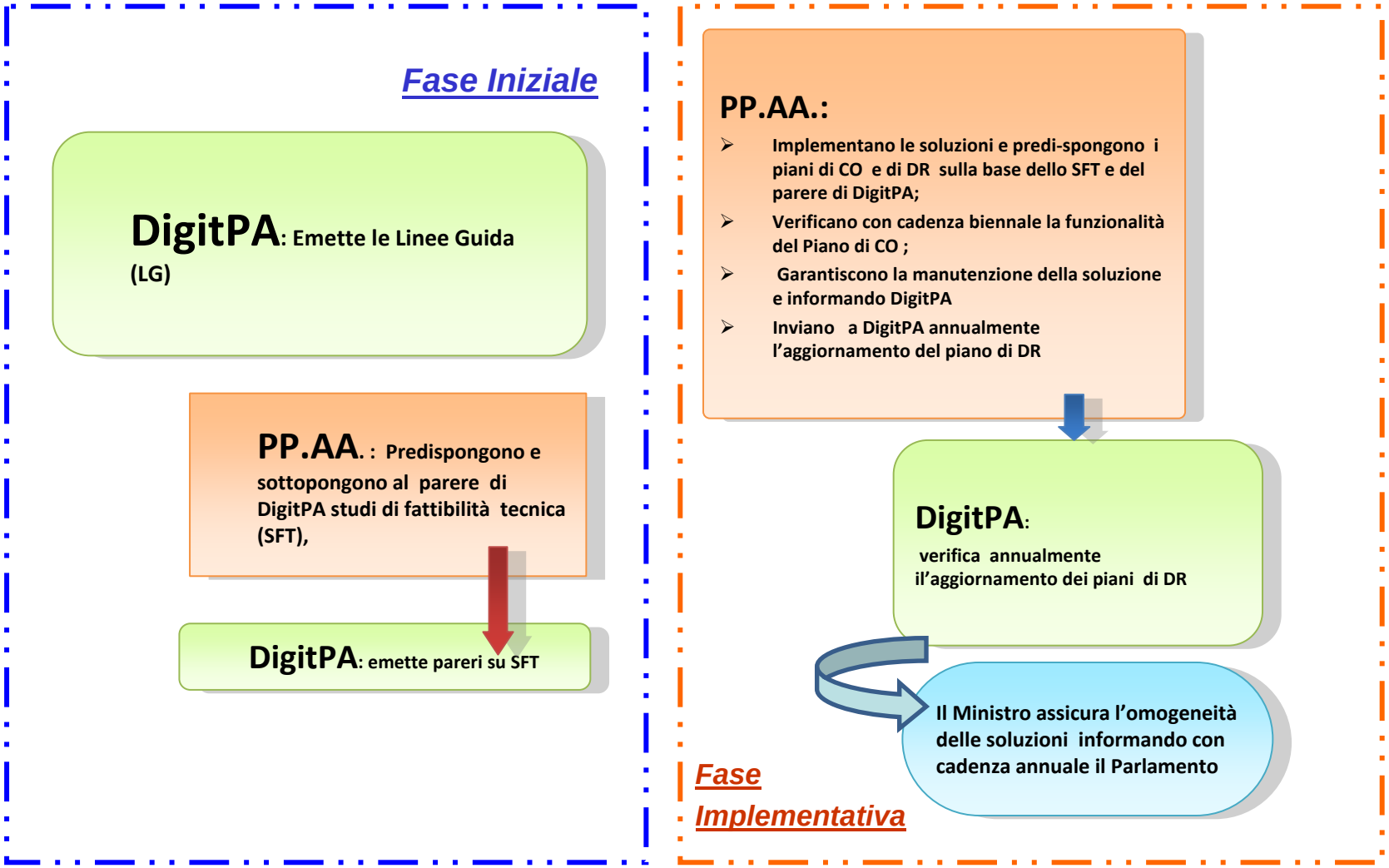
Fase di verifica/controllo per assicurare aggiornamento e omogeneità delle soluzioni

*Verifica annuale, da parte di DigitPA, dei piani di DR e informativa al Ministro.

DigitPA:
- verifica annualmente il costante aggiornamento dei piani di DR;
- ne informa il Ministro.

Il Ministro assicura l'omogeneità delle soluzioni e ne informa, con cadenza annuale, il Parlamento

Workflow previsto /2



Contenuti minimi dello Studio di Fattibilità Tecnica (SFT)

- ***INFORMAZIONI GENERALI***: sono riportate le informazioni generali dell'Amministrazione che emette lo SFT
- ***L'AMBITO DELLO STUDIO DI FATTIBILITÀ TECNICA*** : contiene la descrizione dell'ambito in cui si applica lo Studio, ossia il complesso dei servizi e della relativa struttura che li eroga.
- ***IL RISULTATO DEL PERCORSO DI AUTOVALUTAZIONE :*** in questa parte devono essere riportati i dati emersi nel corso dell'autovalutazione e che sono riportati nello schema di sintesi dell'autovalutazione, ossia:
  - Indice complessivo di criticità;
  - Classe di criticità;
  - Soluzione tecnologica.
- ***LA SOLUZIONE TECNICA:*** in essa viene indicato se i servizi/classe servizi elencati sono coperti da un'unica soluzione o sono previste diverse soluzioni.
- ***TEMPI E MODALITÀ DI REALIZZAZIONE DELLA SOLUZIONE:*** in questa parte vengono riportati i tempi e le modalità di realizzazione delle soluzioni individuate.

Autovalutazione / 1

- Foglio excel “guidato”
- Si basa sulla rilevazione di alcuni specifici parametri, che descrivono gli aspetti significativi di criticità o complessità dell’Amministrazione secondo tre direttrici denominate **servizio, organizzazione** e **tecnologia:**
  - **Servizio:** aspetti legati alla tipologia, numerosità e criticità dei servizi erogati, in termini di danno per l’organizzazione e/o per i suoi utenti in caso di mancata erogazione del servizio stesso
  - **Organizzazione:** aspetti legati alla complessità amministrativa e strutturale dell’organizzazione
  - **Tecnologia:** aspetti legati al fattore tecnologico in termini di dimensione e complessità
- Ciascun parametro viene valutato mediante una **scala qualitativa e quantitativa** costituita da una lista di scelte predeterminate, che rispecchiano le possibili alternative associate al parametro stesso.

Autovalutazione / 2

PAGINA DATI DI SINTESI

Riepilogo degli indici di criticità	
Direttrice	**Valore**
Servizio	3
Organizzazione	2
Tecnologia	5
Indice complessivo di criticità	**3**
Valutazione complessiva	
Classe di criticità risultante	Media
Soluzione tecnologica minima	Tier 3

Generale | Servizio | Organizzazione | Tecnologia | Dati di sintesi

Disater recovery: soluzioni tecniche previste

- **Tier 1** : **backup dati** e conservazione presso un altro sito con **spazi attrezzati per accogliere risorse elaborative** in caso di disastro, con garanzia della disponibilità di risorsa di elaborazione in emergenza

- **Tier 2**: soluzione simile a quella di Tier 1 ma le **risorse elaborative, già presenti**, possono essere disponibili in tempi più brevi

- **Tier 3**: soluzione simile a quella di Tier 2 ma il trasferimento dei dati tra il sito primario e quello di DR avviene attraverso un **collegamento di rete tra i due siti**

- **Tier 4:** la soluzione prevede che **le risorse elaborative**, garantite coerenti con quelle del centro primario, **siano sempre disponibili**, permettendo la ripartenza delle funzionalità in tempi rapidi (**l'aggiornamento dei dati è asincrono**)

- **Tier 5**: la soluzione è analoga a quella del Tier4, con la differenza che l'aggiornamento finale dei dati avviene solo quando entrambi i siti hanno eseguito e completato i rispettivi aggiornamenti (**l'aggiornamento dei dati e' sincrono**)

- **Tier 6:** la soluzione prevede che nel sito di DR le risorse elaborative, oltre ad essere sempre attive, siano funzionalmente speculari a quelle del sito primario, rendendo così possibile ripristinare l'operatività dell'IT in tempi molto rapidi (**erogazione attiva-attiva**)

Stesura dello SFT: articolazione delle fasi

- Individuare i **servizi** che si intende inserire **nel perimetro di analisi**
- Eventualmente raggruppare i servizi individuati in classi omogenee
- Compilare le relative **schede di autovalutazione** e ricavare:
    - l'indice complessivo di criticita'
    - la classe di criticita' risultante (bassa, media, alta, critica)
    - la soluzione tecnologica minima (Tier[1-6])
- **Identificare la soluzione** che si intende adottare e le tempistiche
- Se la soluzione che si intende adottare è diversa dal Tier risultante dall'autovalutazione, **identificare le motivazioni** che vanno specificate nello SFT (soprattutto se la soluzione che si adotta è relativa a un Tier piu' basso rispetto a quello emerso dalla autovalutazione).

Possibili approcci

- A (“coerente”)
  - Individuare il corretto livello di servizio che si ritiene necessario/opportuno garantire
  - Dichiararlo nello SFT
  - Intraprendere le eventuali azioni necessarie per sostenerlo
- B (“tattico”)
  - Individuare il corretto livello di servizio X che si ritiene necessario/opportuno garantire
  - Dichiararne uno inferiore Y nello SFT
  - Intraprendere le eventuali azioni necessarie per garantire X
- C (“propenso al rischio”)
  - Individuare il corretto livello di servizio X che si ritiene necessario/opportuno garantire
  - Dichiararne uno inferiore Y nello SFT
  - Aspettarsi che il sistema, con risorse per Y possa garantire X…

Piano di Continuità Operativa

- **FINALITÀ E AMBITO DI APPLICAZIONE**: dovrebbero esser indicati i servizi da recuperare e le priorità di recupero, i tempi entro i quali i servizi devono essere recuperati (RTO), i livelli di recupero dei dati necessario per ogni servizio (RPO), le condizioni che portano a invocare il piano
- **RUOLI E RESPONSABILITÀ**: dovrebbero essere indicati i ruoli/responsabilità' delle persone e del team che sono coinvolti, in termini di processo decisionale e di livello di autorità durante e dopo un'emergenza
- **MODALITÀ DI ATTIVAZIONE, GESTIONE E MANUTENZIONE DEL PCO**: dovrebbero essere indicate le modalità per mobilitare le persone e i team interessati, la localizzazione dei punti di ritrovo dei team interessati, le circostanze in cui l'organizzazione ritiene che l'attivazione del PCO non sia necessaria, le modalità di gestione, manutenzione e verifica e test del PCO, **il piano di disaster recovery**, le modalità di rientro dall'emergenza

Piano di Disaster Recovery

- FINALITÀ E I CONTENUTI DEL PIANO DI DR
- DESCRIZIONE DELLA SOLUZIONE DI DR
- OBIETTIVI DEL PIANO DI DR
- INFORMAZIONI RELATIVE AL PIANO DI DR
- CLAUSOLE E DIRETTIVE APPLICABILI
- PERIMETRO DI RIFERIMENTO DEL PIANO
- ORGANIZZAZIONE E PERSONALE
- POLITICA DI SICUREZZA E DI SALVAGUARDIA DEI DATI
- FASI DELLA SOLUZIONE DI DISASTER RECOVERY
- GESTIONE DEL PIANO
- COLLEGAMENTI / EVENTUALI INTERAZIONI CON GLI ALTRI DELIVERABLE CONTRATTUALI
- PROCEDURE DI TEST

Incontro 30/01/12: Proposta di articolazione dei servizi

A. Infrastrutttura:
   - Rete elettrica, infrastruttura per garantire la continuità elettrica, condizionamento
   - Rete dati ed apparati, DNS, *[da verificare] firewall*
   - *Layer architetturali necessari per l'erogazione dei servizi applicativi (dbms/application/web server)*
   - *Gestione delle postazioni di lavoro necessarie per la continuità operativa*

B. Servizi telefonici VoIP

C. Identity Management System (AAA - authentication, authorization and accounting)

D. Posta elettronica

E. Sito di Ateneo, Portale dei servizi

F. Cluster di servizi applicativi destinati a supportare i processi di specifici contesti gestionali:
   - Protocollo informatico
   - Gestione del personale (retributivo, giuridico, gestione HR)
   - Contabilità
   - Studenti e didattica
   - Biblioteche
   - Logistica e controllo accessi
   - Ricerca: Catalogo e vetrina dei prodotti della ricerca
   - Servizi di e-learning e di supporto alla didattica
   - *Trouble ticketing / call center*

Incontro 30/01/12: osservazioni /1

1. Per ciascun cluster di servizi applicativi è, in generale, possibile individuare una **partizione tra i servizi** necessari per supportare l'attività di gestione da parte degli uffici ed i servizi erogati online all'utenza (es. studenti, docenti, personale); ciascuna delle due componenti potrebbe avere SLA differenti.
2. E' opportuno che venga compilata una **matrice delle dipendenze tra i servizi** al fine di evidenziare quelli maggiormente critici
3. Atenei diversi potrebbero avere **SLA differenti** per gli stessi servizi
4. E' opportuno evidenziare quali servizi sono soggetti a **scadenze poste da terzi** (es. scadenze normative)
5. Andrebbe fatto un **censimento dei servizi** attivati in Ateneo, non solo dall'Amministrazione ma anche dalle altre strutture (es Dipartimenti), almeno per avere consapevolezza delle implicazioni di eventuali guasti e malfunzionamenti. Si concorda comunque di escludere dal perimetro di analisi dello SFT i servizi in hosting presso i Dipartimenti (e a maggior ragione quelli erogati dagli stessi per conto terzi).

Incontro 30/01/12: osservazioni /2

6. Il **modello di autovalutazione** (destinato alla determinazione della soluzione tecnologica) si dimostra molto “sensibile” ai parametri dimensionali dei servizi valutati (es. num DB) ed agli SLA (es tempo di ripristino) => è necessario tenerne in debito conto nella definizione dei servizi e nella compilazione
7. E’ opportuno che i **costi** implicati dalle esigenze di continuità operativa e disaster recovery vengano esplicitati sottolinenandone, in sede di preparazione dei budget, “l’incomprimibilità”.
8. I tempi di ripristino potrebbero essere differenziati sulla base della **fascia oraria** (in orario lavorativo piuttosto che notturno/festivo)
9. E’ necessario che del **Comitato di gestione della crisi** faccia parte anche il Direttore Generale/Amministrativo
10. Policy di **hosting CINECA**