"Censimento del Patrimonio ICT della PA":
Indicazioni di massima sulla compilazione formulate dal Gruppo ICT del CODAU

Premesse

a. AgID ha confermato che questa fase del censimento http://www.agid.gov.it/notizie/2018/04/13/piano-triennale-dal-23-aprile-al-seconda-fase-del-censimento-del-patrimonio-ict riguarda anche le Università: https://helpdeskcensimentoict.italia.it/knowledgebase.php?article=2 *"La seconda fase del Censimento è rivolta a tutte le Pubbliche Amministrazioni ed è stata avviata il 23 aprile con la pubblicazione online sul sito Web dedicato all'iniziativa delle modalità di svolgimento e delle istruzioni operative.",* quindi AgID non invierà alcuno specifico invito alle PA coinvolte per avviare la procedura.

b. La compilazione del questionario di rilevazione è di competenza del Responsabile per la transizione digitale o, nel caso in cui non risultasse ancora nominato, di un incaricato con nomina formale a "Responsabile del Censimento del Patrimonio ICT".

c. Per ciascun Ateneo è prevista la compilazione di un solo questionario, associato al suo Codice IPA.

d. Si concorda, ai fini del censimento, di non prendere in considerazione data center / locali tecnici / infrastrutture / risorse dislocate presso i Dipartimenti e da loro gestite. Ciò vale in termini generali, per alcuni Atenei nei quali i Dipartimenti hanno in dotazione infrastrutture significative (es data center di medie dimensioni) potrebbero essere opportune scelte differenti.

e. La sezione finale sulle "Voci di spesa" è opzionale e deve essere compilata solo per candidatura a PSN => non ci riguarda

Osservazioni alle domande del questionario di censimento

I punti sono numerati in coerenza con le corrispondenti domande del questionario.

- **13. Numero di sedi dell'Ente**

  Si concorda di tenere come riferimento il numero di Sedi dichiarate al MIUR (es. Campus metropolitani + Poli territoriali).

- **16. Numero di addetti ICT interni all'Ente**

  Si concorda di conteggiare tutto il personale strutturato dell'Ateneo con mansioni certificate/formali in ambito ICT, incluso quello con afferenza dipartimentale (es: referenti per l'ICT di dipartimento, nuclei tecnici di supporto interno alle singole strutture). Ciò per dare maggior peso alla struttura complessiva d'Ateneo dedicata all'erogazione dei servizi.

  Peraltro il personale dei Dipartimenti potrebbe effettivamente essere impiegato nella gestione di servizi/macchine in hosting/housing presso i data center dell'Amministrazione.

  Notare il fatto che l'esclusione dal conteggio degli FTE esterni potrebbe portare ad una sottostima delle risorse effettivamente dedicate all'erogazione di servizi.

- **19. L'Ente è conforme alle normative riportate in elenco?**
  - UNI EN ISO 9001 (gestione della qualità)
  - Eco-management and Audit Scheme
  - ISO 14001 (gestione ambientale)
  - ISO 18001 (Gestione della sicurezza e della salute dei lavoratori)
  - ISO 20000 (Gestione servizi IT)

  Usualmente gli Atenei non hanno tali certificazioni, alcuni potrebbero forse essere conformi ma non certificati. **[Quesito aperto]** Per ISO 9001, considerato che è riferito all'Ente nel suo complesso va inteso come: tutti i processi sono certificati e non solo alcuni?

- **20. Indicare se esistono i seguenti piani e meccanismi di governance**
  - Processo di analisi del rischio e privacy impact assessment => SI x GDPR
  - Processo di gestione degli incidenti ICT (cd. Data Breach) => SI x GDPR
  - Piano di sicurezza informatica => SI, vedi MMS di AgID
  - Piano Formazione e Comunicazione sui Sistemi Informativi => verificare formazione con Risorse Umane
  - Comitato di gestione e pianificazione dei sistemi informativi con aggiornamenti periodici sui processi di governance IT => es presenza di un delegato del Rettore e/o vero Comitato tecnico-scientifico o di gestione e/o momenti formali di coordinamento anche con scadenze variabili.

- **28. Indicare come l'Amministrazione si assicura la connessione ad Internet**
  - Tramite fornitore di accesso privato (ISP Privato)
  - Tramite fornitore di accesso pubblico (SPC) => SI
  - Tramite fornitore di accesso pubblico in house => SI, GARR

- **37. L'Ente fornisce "punti di accesso" Wi-Fi gratuiti sul proprio territorio?**

  Si conviene di considerare tale l'accesso dato gratuitamente a studenti, docenti e personale tecnico-amministrativo, anche tramite autenticazione federata IDEM o Eduroam.

- **38. Numero medio mensile di cittadini che usano il Wi-Fi messo a disposizione dall'Ente**

  Si conviene di conteggiare gli accessi da parte di tutti gli utenti sia interni che esterni all'Ateneo autenticati tramite IDEM o Eduroam, oltre naturalmente a soluzioni basate su SPID.

- **44. Indicare le applicazioni informatiche che supportano "funzioni critiche" per i cittadini, le imprese o altre PPAA**

  Le istruzioni specificano che: "*un'applicazione è da considerarsi "critica" quando, nel caso in cui dovesse smettere di funzionare anche solo per pochi minuti, comporterebbe per la PA una perdita di denaro o di immagine, e/o un danno (materiale e/o immateriale) da parte degli utenti finali del servizio (es. cittadini e/o imprese e/o altre PA), oltre che, in caso di evento catastrofico, concorrere ad un ritardo nelle operazioni di soccorso.*".
  - Nel caso degli Atenei servizi con SLA così stringenti sono rari.
  - Per l'individuazione delle applicazioni si ipotizza, in prima battuta, di far riferimento agli ambiti ed agli SLA individuati in sede di redazione dello Studio di fattibilità per il Piano di continuità operativa.

    Si potrebbe partire da quelli e considerare solo quelli più critici (ovvero con valori di RTO e RPO più bassi).

    Ad esempio PoliMI aveva indicato:

Servizio	SLA
Identity management	24x7 RPO 1h RTO 1h
Posta Elettronica	24x7 RPO 1h RTO 1g
Portale di Ateneo	24x7 RPO 4h RTO 1g
Gestione personale	24x7 RPO 1h RTO 1g
Gestione studenti	24x7 RPO 1h RTO 1g
Contabilità	24x7 RPO 1h RTO 1g
Gestione catalogo della ricerca	24x7 RPO 1h RTO 1g
Logistica e accessi	24x7 RPO 1h RTO 1g
Protocollo	24x7 RPO 1h RTO 1g

Servizi bibliotecari	24x7 RPO 1h RTO 1g

- Valutare se non sia opportuno aggiungere, tra i servizi erogati dall'Amministrazione, anche quelli di calcolo e storage offerti ai Dipartimenti (hosting di servizi e/o housing di hw nei data center dell'Amministrazione). E' vero che sono esterni al perimetro di indagine definito nello Studio di fattibilità per il Piano di continuità operativa, tuttavia, ai sensi della Circolare AgID 5 del 30/11/17:

  Sono esclusi dalla richiesta di approvazione gli adeguamenti che prevedono acquisti nei seguenti ambiti:
  - progetti di ricerca a titolarità di istituzioni universitarie e/o enti di ricerca;

  , sono gli unici servizi che possono costituire un'eccezione rispetto alle indicazioni del Piano triennale ICT per la PA.

  A riguardo è opportuno ricordare che i nostri Studi di Fattibilità per BC&DR avevano ricevuto da AgiD parere favorevole condizionato all'inserimento anche dei servizi Dipartimentali.

- Per gli Atenei che abbiano i servizi dichiarati in hosting/SaaS presso CINECA, gli SLA da dichiarare sono disponibili sul wiki di Cineca (si veda anche il punto successivo).
- Non vengono richiesti livelli SLA per il singolo servizio sia che si dichiari il servizio critico on premise o in ASP/SaaS. I livelli di servizio sono riferiti solo al DC (nel caso di servizi critici in SaaS o ASP l'informazione viene rilevata quindi mai)
- Servizi critici "tipici" per le Università, es. IDM o posta elettronica, Catalogo della ricerca" non sono previsti e nella selezione di "servizio/funzione amministrativa principale supportata dall'applicazione" devono essere etichettati come "Nessuna delle precedenti".

  Per quanto riguarda i servizi bibliotecari, l'unica opzione è "Consultazione OPAC SBN" per gli Atenei che utilizzano soluzioni diverse e non sono polo SBN utilizzare "Nessuna delle precedenti".

- **51. Numero di Data Center dell'Ente e/o aree dedicate ai server "di proprietà dell'Ente" e "presso terzi Data center**

  [Quesito aperto] Si considera DC anche la sala destinata esclusivamente al backup?

  Nel caso di strutture fisiche separate potrebbe essere considerata tale (es. primario, DR, backup)

- **53a. Indicare se l'Ente fa uso di servizi di hosting – allegato tecnico Cineca (schede di hosting) contiene tutti i dettagli delle SLA (Range, non su singoli servizi)**
  - No, l'Ente non fa uso di servizi di hosting
  - L'Ente utilizza servizi di hosting forniti da un CST (Centro Servizi Territoriali) o da un soggetto esterno a partecipazione pubblica => SI, CINECA e/o Società di sistema locali.
  - L'Ente utilizza servizi di hosting forniti da un'altra PA
  - L'Ente utilizza servizi di hosting forniti da un soggetto esterno privato

- **57. Localizzazione del Data Center**
  - *Struttura dedicata*
  - *Modulo container/Security Room*
  - *Stanza dedicata al server presso l'Ente*

  Se si sceglie l'opzione "Stanza dedicata al server presso l'Ente" il questionario richiede un numero ridotto informazioni aggiuntive relative agli impianti tecnici.

  [Quesito aperto] "Struttura dedicata" vs "Stanza dedicata al server presso l'Ente" quando, pur non essendo l'edificio esclusivamente dedicato al DC, sia dotato di impianti tecnici ad hoc?

  [Quesito aperto] Selezionare l'opzione "Stanza dedicata al server" prefigura un'attribuzione in "classe B"?

- **65. Numero totale di personale tecnico interno addetto alla gestione del Data Center**

  Si concorda di includere non solo il personale dedicati alla gestione fisica dei Data Center ma anche quello addetto alla rete ed ai servizi di hosting.

[Quesito aperto] Concordiamo di conteggiare "unità di personale" e non FTE in senso stretto?

- **68. Indicare le fasce orarie di presidio tecnico presso il Data Center**
  - Ventiquattro ore su ventiquattro (h24)
  - Dal lunedì al venerdì (orario ufficio)
  - Orario ufficio e sabato, domenica e festivi con orario ridotto
  - Altre fasce orarie (specificare)

  Si concorda di considerare equivalente al presidio in presenza del Data Center la copertura in reperibilità h24 7/7 purché contrattualmente definita con SLA adeguati.

- **69a. Informazioni sulla struttura del Data Center (2/2)**

  Indicare la superficie di hosting totale (in mq) del Data Center (esclusa la superficie dedicata alle postazioni di lavoro)

  [Proposta] Consideriamo la superficie totale dei locali

  Indicare la superficie di hosting occupata (in mq) del Data Center (esclusa la superficie dedicata alle postazioni di lavoro)

  [Proposta] Consideriamo l'impronta a terra dai rack, escluso lo spazio di accesso

- **87. Indicare la superficie media (in mq) per rack (intesa come spazio del rack più lo spazio per l'accesso al rack)**

- **89. Indicare la superficie (in mq) disponibile nel Data Center per la co-location di unità rack**

  [Proposta] Consideriamo la superficie disponibile per la collocazione dei rack, escluso lo spazio di accesso/manovra agli stessi .

- **91. Per ciascuna tipologia di server in elenco fornire le seguenti informazioni**

  Ultimo aggiornamento del Sistema Operativo (anno)

  [Quesito aperto]Cosa si intende con "ultimo aggiornamento"? L'ultima patch applicata o l'ultima versione di s.o. installata?

  [Quesito aperto] Trattandosi di un dato riferito ad un insieme di server con policy di aggiornamento diverse, prendiamo la meno recente?

- **90. Selezionare le tipologie di server presenti nel Data Center**

  [Quesito aperto] Tenendo conto che si parla di server presenti considerare anche eventuali appliance?

- **102. Indicare la dimensione complessiva dello storage espresso in Tera Bytes (TB) del Data Center**

  [Quesito aperto] Considerare il totale raw, includendo le repliche e non considerando RAID?

- **103. Indicare la/le tecnologia/e (NAS, SAN, ecc.) utilizzata/e per lo storage del Data Center**

  Scegliere solo una delle seguenti voci:
  - *NAS*
  - *SAN*
  - *Altra tecnologia di storage (specificare)*

  [Quesito aperto] Nel caso vengano utilizzate molteplici tecnologie, elencarle tutte nell'opzione "Altro"?

- **120. Il Data Center garantisce il rispetto dei requisiti delle seguenti norme/standard?**

  Vedere punto 19

- **121. Indicare quali dei seguenti piani/procedure e/o meccanismi di governance sono stati approvati e adottati formalmente**

- Processo di analisi del rischio e privacy impact assessment => SI x GDPR
- Piano di disaster recovery => SI, vedi BC/DR AgID
- Piano di continuità operativa (formalmente approvato) => SI, vedi BC/DR AgID
- Procedure operative da attivare in caso di indisponibilità parziale dei servizi applicativi ospitati nel Data Center
- Piano di sicurezza informatica => SI, vedi MMS di AgID
- Procedura di gestione della configurazione => SI, vedi MMS di AgID
- Processo di gestione degli incidenti ICT (c.d. Data Breach) => SI x GDPR
- Processo di Change Management