Procedura per la verifica dell'idoneità di una infrastruttura all'utilizzo da parte di PSN

UNIONE EUROPEA
Fondo Sociale Europeo
Fondo Europeo di Sviluppo Regionale

Agenzia per la Coesione Territoriale

Dipartimento della Funzione Pubblica

PON GOVERNANCE E CAPACITÀ ISTITUZIONALE 2014-2020

AGID Agenzia per l'Italia Digitale

PROCEDURA PER LA VERIFICA DELL'IDONEITÀ DI UNA INFRASTRUTTURA ALL'UTILIZZO DA PARTE DI PSN

Il presente documento descrive la procedura per la verifica delle infrastrutture candidate a essere utilizzate da PSN a seguito della pubblicazione della circolare Agid n.1/2019 del 14 giugno 2019 (G.U n. 152 del 1/7/2019), alla quale si rimanda per le definizioni e gli acronimi citati in questo documento.

La procedura di valutazione dell'idoneità di una infrastruttura all'utilizzo da parte di PSN, è attuata da AgID attraverso uno o più specifici *Gruppi di Verifica* (nel seguito GdV), composti da un numero variabile di membri, anche esterni, in possesso di diverse competenze specialistiche in relazione alle differenti esigenze che dovessero manifestarsi.

Il coordinamento amministrativo e gestionale delle attività dei GdV è svolto da Agid.

Nel documento *"Modalità operative per la verifica dell'idoneità di un'infrastruttura all'utilizzo da parte di PSN"*, pubblicato a cura di Agid sul proprio sito istituzionale, sono dettagliate le procedure per la costituzione dei GdV, per l'effettuazione delle operazioni di verifica, per la redazione e i contenuti dei documenti e verbali di tracciatura della verifica. Ai GdV potranno anche essere affidate, successivamente alle attività per la verifica dell'idoneità delle infrastrutture, funzioni di controllo del mantenimento delle caratteristiche abilitanti delle stesse infrastrutture.

La valutazione è effettuata sulle infrastrutture risultate preliminarmente idonee a seguito delle fasi di censimento di cui alla circolare Agid 1/2019, attraverso visita in loco e in contraddittorio con l'Amministrazione referente della infrastruttura in verifica.

Le verifiche *in loco* saranno condotte secondo i princìpi della norma UNI EN ISO 19011:2018.

La procedura di verifica si svolge secondo le seguenti fasi:

1. Agid, in occasione della comunicazione finale dell'esito del censimento di cui alla circolare Agid 1/2019, richiede all'Amministrazione referente di una infrastruttura ritenuta candidabile a essere utilizzata da PSN, la manifestazione della volontà di sottoporre alla verifica tale infrastruttura; nel caso che l'Amministrazione non confermi tale volontà, l'infrastruttura è classificata come Gruppo A (vedasi richiamata circolare Agid 1/2019);

2. Costituzione del (o dei) GdV, a cura di Agid;

3. Comunicazione di Agid all'Amministrazione referente dell'infrastruttura della data della visita in loco, almeno 15 giorni solari precedenti tale data. La comunicazione contiene:

    a. la composizione del GdV;
    b. documenti e strutture da rendere disponibili a cura dell'Amministrazione per la verifica;
    c. data di inizio delle attività di verifica e modalità di svolgimento;
    d. stima del tempo e della durata delle attività;

4. l'Amministrazione comunica ad Agid, entro 7 giorni solari dal ricevimento della comunicazione al punto 3. precedente, il referente dell'Amministrazione per la verifica e i nominativi e le qualifiche del personale partecipante per l'Amministrazione alla verifica; passato questo periodo senza il ricevimento di queste indicazioni da parte dell'Amministrazione o di ricevimento parziale delle informazioni richieste, non si procede ai passi ulteriori e l'infrastruttura è classificata come Gruppo A;

5. il gruppo di verifica effettua la visita in loco. Tale visita si svolge in tre distinti momenti:

    a. verifica dell'effettiva conformità ai requisiti preliminari di cui all'allegato A della circolare 1/2019 di Agid;
    b. verifica dei riscontri documentali;
    c. verifica dei requisiti infrastrutturali complementari

    Relativamente alla verifica al punto a., e in particolare relativamente alle procedure previste ai punti 1., 2., 3. della tabella presente nell'allegato A alla circolare 1/2019 di Agid, l'Amministrazione referente dell'infrastruttura deve possedere, o presentare un piano di adeguamento, già avviato al momento della verifica, al fine di ottenere le seguenti certificazioni ISO 20000-1:2011, ISO 27001:2013, ISO 22301:2012 (versioni riportate o successive). Nell'allegato B alla presente procedura sono indicati, sempre in riferimento alle procedure previste ai punti 1., 2., 3. della tabella presente nell'allegato A alla circolare 1/2019 di Agid, i contenuti minimi che, in assenza di possesso delle certificazioni relative, tali procedure devono comunque prevedere e che saranno oggetto di riscontro;

6. nel caso di riscontro negativo al termine delle fasi a. e b., la verifica si interrompe, il Gruppo di Verifica comunica all'Amministrazione le non conformità riscontrate e l'Amministrazione ha tempo 15 giorni solari dalla comunicazione per informare Agid di avere rimosso tali non conformità e richiedere una nuova verifica;

7. entro 7 giorni solari dalla eventuale richiesta del punto precedente, Agid comunica la data di nuova visita perriprendere l'esame degli elementi non conformi;

8. nel caso di esame di cui al punto precedente con esito positivo, la visita prosegue secondo i passi del precedente punto 5. Nel caso di ulteriori riscontri negativi, la procedura di verifica si interrompe definitivamente e l'infrastruttura è classificata come Gruppo A o Gruppo B, al termine della verifica relativamente al precedente punto 5.a oppure è classificata come Gruppo A, al termine della verifica relativamente al precedente punto 5.b;

9. nell'allegato A alla presente procedura sono riportati i requisiti infrastrutturali complementari oggetto di verifica (precedente punto 5. c), unitamente ai valori (o intervallo di valori) attesi per ogni requisito e all'indicazione dei requisiti ritenuti essenziali; il non possesso dei requisiti essenziali implica il non superamento della verifica e la non iscrizione dell'infrastruttura nell'elenco delle infrastrutture idonee a essere utilizzate da PSN; l'infrastruttura viene classificata come Gruppo A. Si precisa che la stessa infrastruttura deve presentare un piano di gestione del rischio sismico e idrogeologico (come richiesto dal Piano di continuità operativa).

10. al termine della verifica, qualunque sia la fase che conclude la stessa verifica, viene stilato un verbale firmato dal GdV e dall'Amministrazione che precisa tutte le attività svolte e, puntualmente, l'esito dei riscontri effettuati in relazione alla fase di verifica effettuata. In caso di conclusione positiva di tutte le fasi della verifica, il GdV produce una relazione complessiva dell'attività di verifica, contenente la proposta di iscrizione dell'infrastruttura nell'elenco di quelle idonee a essere utilizzate da PSN

11. a seguito della relazione del precedente punto 10., Agid valuta la stessa e, se approvata, iscrive l'infrastruttura esaminata nell'elenco delle infrastrutture idonee a essere utilizzate da PSN

12. é richiesta la ridondanza dei sistemi di connettività di rete dell'infrastruttura tramite l'utilizzo di almeno due distinti carrier in ingresso al datacenter (connettività multi-carrier).

ALLEGATO A

Requisiti infrastrutturali complementari oggetto di verifica

N°	Ambito	Indicatore	Valutazione	Requisito essenziale	Requisito non essenziale (preferibile)
1	Architettura - Sito geografico	Prossimità del CED a corsi d'acqua	Maggiore di 91 m	X	
2	Architettura - Sito geografico	Prossimità del CED ad arterie autostradali/ferroviarie	Maggiore di 91 m	X	
3	Architettura - Sito geografico	Prossimità del CED ad aeroporti	Maggiore di 1,6 km	X	
4	Architettura - Parcheggio	Prossimità del parcheggio visitatori ai muri perimetrali del CED	Barriere di protezione per impedire la collisione di un veicolo con il muro esterno delle aree di facility e computer room distante almeno 9.1 m		X
5	Architettura - Parcheggio	Parcheggio dipendenti separato da quello visitatori	Sì, fisicamente separati da una recinzione o da un muro con ingressi separati		X
6	Architettura - Parcheggio	Area carico/scarico separata dal parcheggio	Sì, fisicamente separati da una recinzione o da un muro con ingressi separati, o mediante un sistema con controllo accesso fisico, in modo da eliminare le interferenze fra le operazioni di carico/ scarico e il passaggio di auto	X	
7	Telecomunicazioni - Generale	Area principale di distribuzione telecomunicazioni ridondata	Sì	X	
8	Telecomunicazioni - Generale	Cablaggi telecomunicazioni e percorsi orizzontali ridondanti	Sì	X	
9	Telecomunicazioni - Generale	Pozzetti di Accesso della fibra con distanza superiore ai 20 m	Sì	X	
10	Telecomunicazioni - Generale	Ridondare l'area dedicata all'attestazione della fibra con gli apparati dei carrier/provider provenienti dai pozzetti di ingresso con la logica di collegamento diretto e incrociato	Sì		X
11	Telecomunicazioni - Generale	Router e Switch hanno alimentatori e control station ridondati	Sì	X	
12	Telecomunicazioni - Generale	Router ridondanti e switch con uplink ridondato	Sì	X	
13	Architettura - Componenti costruttive	Tipo di pannelli del pavimento rialzato (se presente)	Pannelli con opportuna capacità di carico (es. Solfato di Calcio)		X
14	Architettura - Componenti costruttive	Accoppiamento pannello e sottostruttura (quando il pavimento rialzato è presente)	Struttura con resistenza al carico di almeno 1600 Kg/mq		X
15	Architettura - Corridoi di uscita	Separazione antincendio corridoi di uscita dalla sala computer e dalle aree di supporto	Secondo le normative, non inferiore a REI 60	X	
16	Architettura - Corridoi di uscita	Larghezza dei corridoi di uscita	secondo le normative, non inferiore a 1,2 m		X
17	Architettura - Area di spedizione/ ricezione	Area spedizioni separata fisicamente dalle altre aree del Data Center	Sì	X	

N°	Ambito	Indicatore	Valutazione	Requisito essenziale	Requisito non essenziale (preferibile)
18	Architettura - Area di spedizione/ricezione	Numero di banchine di carico in area di spedizione/ricezione	Minimo 1	X	
19	Architettura - Locali di stoccaggio combustibile e generatori	Prossimità locali di stoccaggio combustibile e generatori alle sale dati ed alle aree di supporto	Se all'interno dell'edificio, dotato di compartimentazione REI 120 al minimo con eventuali prescrizioni VVFF, se all'esterno secondo le prescrizioni dei VVFF	X	
20	Architettura - Sicurezza	Sistema di controllo (TVCC, Accessi, Antiintrusione), dispositivi in campo e apparati di visualizzazione sotto continuità	UPS dedicato al sistema di controllo e visualizzazione oppure batterie locali sui dispositivi di campo, con autonomia di 8 ore	X	
21	Architettura - Sicurezza	Personale di sicurezza fisica	24h/7gg	X	
22	Architettura - Controllo accessi	Controllo accessi ai varchi di tutte le sale del Data center, compresa l'entrata principale	Entrata e uscita con badge o biometrico, sistema antiintrusione, allarme porta/ finestra aperta	X	
23	Architettura - Strutturale	Rack / armadi di apparecchiature per telecomunicazioni fissati alla base o supportati in alto e alla base o dotato di piattaforme sismiche o altre misure protettive	Sì	X	
24	Architettura - Ingresso edificio	Ingresso dell'edificio con guardiola e bancone della sorveglianza per il controllo dei documenti e delle autorizzazioni, adeguatamente protetto (requisito di vetro anti proiettile livello 3)	Sì	X	
25	Architettura - Ingresso edificio	Ingresso dell'edificio con porte e finestre antincendio	Almeno REI 60 (se presente permesso specifico rilasciato dai VVFF è considerato conforme)	X	
26	Architettura - Ingresso edificio	Ingresso edificio con porte interbloccate con accesso singolo, sistemi fisici anti scavalcamento e anti passback	Si	X	
27	Architettura - Uffici amministrativi	Uffici amministrativi separati dall'area del CED	Sì	X	
28	Architettura - Aree del personale	Prossimità di servizi igienici o sale ristoro alle sale dati	Adiacenti con antiallagamento	X	
29	Architettura - Aree del personale	Separazione antincendio dei servizi igienici e sale ristoro dalle sale dati e dalle aree di supporto	Almeno REI 60	X	
30	Architettura - Videosorveglianza	Controllo TVCC a tutte le aree ristrette con accesso tramite porte con badge	Sì	X	
31	Architettura - Videosorveglianza	TVCC dei varchi con controllo d'accesso	Sì	X	
32	Architettura - Videosorveglianza	Registrazione TVCC di tutte le attività su tutte le telecamere	Si, in digitale (mantenimento delle registrazioni di almeno 30 giorni)	X	
33	Architettura - Videosorveglianza	Frequenza immagini TVCC (framerate)	20 frame/sec o più		X
34	Elettrico - Generale	Il sistema di distribuzione elettrica consente la manutenzione a caldo	Sì, senza esclusioni	X	
35	Elettrico - Generale	Analisi del sistema elettrico	Relazione di progetto che dovrà comprendere il calcolo delle potenze di corto circuito, studio di coordinamento verticale, analisi dell'arco elettrico e studio del flusso di carico	X	

N°	Ambito	Indicatore	Valutazione	Requisito essenziale	Requisito non essenziale (preferibile)
36	Elettrico - Generale	Cavi elettrici per computer e apparecchiature per telecomunicazioni	Cavi di alimentazione ridondanti con capacità del 100% sui rimanenti cavo o cavi	X	
37	Elettrico - Sistemi UPS	Ridondanza sistemi UPS	N+1	X	
38	Elettrico - Sistemi UPS	Bypass automatico e bypass di manutenzione	Bypass automatico alimentato con interruttore dedicato e presenza di interruttore di bypass esterno per esclusione totale UPS	X	
39	Elettrico - Sistemi UPS	Distribuzione elettrica in uscita dai sistemi UPS	Quadro elettrico con interruttori estraibili con funzioni adjustable long time e instantaneous trip	X	
40	Elettrico - Sistemi UPS	Tipo di batterie dei sistemi UPS	Batterie progettate per 5-10 anni di vita media con UPS statici oppure UPS rotanti	X	
41	Elettrico - Sistemi UPS	Durata minima delle batterie dei sistemi UPS	10 minuti con UPS statici o UPS rotanti	X	
42	Elettrico - Sistemi UPS	Sistema di monitoraggio delle batterie dei sistemi UPS	Monitoraggio gestito dall'UPS a livello dei banchi	X	
43	Elettrico - Sistemi UPS	Topologia sistemi UPS	Ridondanti, distribuiti su moduli o blocchi	X	
44	Elettrico - Commutatore statico	Procedura di bypass per manutenzione del commutatore statico	Manuale guidata con dispositivo di blocco meccanico	X	
45	Elettrico - Distribuzione	Trasformatore	K-Rated / Harmonic Canceling, (o tecnologia equivalente) ad efficienza elevata	X	
46	Elettrico - Scariche Atmosferiche	Impianto di protezione dalle scariche atmosferiche	Sì	X	
47	Elettrico - Messa a terra	Messa a terra delle masse metalliche in Computer Room	Sì	X	
48	Elettrico - Monitoraggio centralizzato	Punti monitorati	Rete elettrica pubblica, Trasformatore principale, UPS, Generatore, Stato Interruttori, STS, ATS, PDU	X	
49	Elettrico - Monitoraggio centralizzatoa	Metodo di notifica degli allarmi	Sala di controllo, cercapersone, Email e/o SMS	X	
50	Elettrico - Locali batterie	Locale batterie separato dal locale UPS	Non obbligatorio a meno che non sia richiesto espressamente dai VVFF. La separazione è comunque preferibile.		X
51	Elettrico - Locali batterie	I singoli gruppi di batterie sono isolati fra loro	Sì	X	
52	Elettrico - Generatori di backup	Dimensionamento dei generatori elettrici automatici di backup (Standby generating system)	Dimensionati per il carico dell'intero edificio con ridondanza N+1	X	
53	Elettrico - Generatori di backup	Generatori su singola barratura	Sì	X	
54	Elettrico - Load bank	Disponibilità Load bank (di proprietà o in affitto)	Portatile	X	
55	Elettrico - Testing	Esecuzione test di accettazione in fabbrica (FAT) apparati elettrici	UPS e generatori	X	
56	Elettrico - Testing	Procedura di collaudo in produzione apparati elettrici	A livello di componenti e di sistema	X	
57	Elettrico - Manutenzione apparati	Personale operativo e di manutenzione apparati elettrici	Onsite 24 ore su 7 giorni	X	
58	Elettrico - Manutenzione apparati	Manutenzione preventiva apparati elettrici	Generatore e UPS	X	

N°	Ambito	Indicatore	Valutazione	Requisito essenziale	Requisito non essenziale (preferibile)
59	Elettrico - Manutenzione apparati	Programma di formazione del personale operativo	Formazione completa per regolare esercizio degli apparati	X	
60	Meccanico - Generale	Ridondanza degli apparati meccanici (es. unità di condizionamento, dry cooler, pompe, torri evaporative, condensatori). I requisiti di ridondanza si applicano anche alle aree di supporto che non sono critiche alla continuità delle operazioni della computer room	Ridondanza N+1 allo scopo di garantire le operazioni di manutenzione a caldo. La perdita temporanea di alimentazione elettrica o di acqua (dove applicabile) non provoca l'indisponibilità del raffreddamento, ma può causare l'innalzamento della temperatura entro i livelli di operatività degli apparecchi critici/essenziali. Le manovre per garantire la manutenzione a caldo possono essere manuali.	X	
61	Meccanico - Generale	Passaggio di tubazioni non attinenti al data center all'interno dello spazio data center	non permesso	X	
62	Meccanico - Generale	La pressione all'interno della Computer Room e nelle aree pertinenti alla Computer Room deve essere maggiore di quella delle altre aree	Sì		X
63	Meccanico - Generale	Pozzetti di scarico, in Computer Room, per la condensa, per gli eventuali apparati di umidificazione e per l'impianto sprinkler, se presente	Sì	X	
64	Meccanico - Generale	Sistemi meccanici alimentati da gruppo elettrogeno in mancanza di rete pubblica	Sì	X	
65	Meccanico - Generale	Controllo dell'umidità nella Computer Room	Sì	X	
66	Meccanico - Sistemi raffreddati ad acqua	Unità interne	Aggiungere un'unità in ridondanza ogni 5-8 unità installate		X
67	Meccanico - Sistemi raffreddati ad acqua refrigerata e ad aria	Alimentazione elettrica agli apparati meccanici	N+1 configurata per garantire la manutenzione a caldo	X	
68	Meccanico - Sistema di controllo HV AC	Sistema di controllo HV AC	Progettato per manutenzione a caldo	X	
69	Meccanico - Sistemi condensati ad acqua	Ripristino livello acqua dei circuiti	Due punti di connessione alla rete di alimentazione dell'acqua	X	
70	Meccanico - Carburante per i generatori	Quantità di carburante	Per garantire un'autonomia di 48 ore (previo possesso di permesso specifico rilasciato dai VVFF)	X	
71	Meccanico - Carburante per i generatori	Serbatoi	Multipli		X
72	Meccanico - Carburante per i generatori	Pompaggio carburante e tubazioni	Per ogni generatore	X	
73	Meccanico - Anti Incendio	Impianto Sprinkler per rilevazione e spegnimento dell'incendio nella parte uffici dell'edificio, o secondo le prescrizioni dei VVFF	Sì		X
74	Meccanico - Anti Incendio	Rilevazione Fumi VESDA per Computer Room ed Entrance Room con presenza di apparati attivi o sistema equivalente	Del tipo pre action con valvola comandata dalla rilevazione	X	
75	Meccanico - Anti Incendio	Spegnimento automatico a gas per Computer Room ed Entrance Room con presenza di apparati attivi	Sì	X	
76	Meccanico - Anti allagamento	Sistema di rilevazione in Computer Room ed Entrance Room con presenza di apparati attivi	Sì	X	

ALLEGATO B

Contenuti minimi per le procedure inerenti i punti 1., 2., 3., della tabella presente nell'Allegato A alla circolare Agid 1/2019

Con particolare riferimento alle verifiche sulla conformità delle infrastrutture delle Amministrazioni ai requisiti dei punti 1.,2., 3. dell'allegato A alla circolare 1/2019 di Agid, si riportano i contenuti minimi attesi. In caso di possesso della certificazione, tali verifiche sulla conformità non sono effettuate da parte del Gruppo di Verifica.

1. Procedure attese delle PA vs ISO 20000

Livello 1	Livello 2	Controllo	Descrizione
Processi per l'erogazione del servizio	Gestione dei livelli di servizio	Processo di gestione dei Livelli di Servizio	Descrizione formale del processo di gestione dei livelli di servizio.
		Service Level Agreement (SLA)	Accordo formale tra l'organizzazione IT e il cliente. Descrive i ruoli e le responsabilità di entrambe le parti, così come gli obiettivi che devono essere raggiunti e caratteristiche del carico di lavoro e eccezioni.
		Reporting del servizio	Documento che fornisce dettagli sui servizi, prestazioni, incidenti, problemi, cambiamenti, ecc.
	Gestione della capacità	Processo di gestione delle capacità	Descrizione formale del processo di gestione della capacità.
		Piano delle capacità	Si deve creare, attuare e tenere aggiornato un piano delle capacità che tenga conto delle risorse umane, tecniche, informative e finanziarie.
		Misure di capacità e prestazioni	Report sulle prestazioni dei servizi e/o componenti utilizzati da altri processi per garantire le prestazioni, e la conformità ai livelli di servizio.
	Gestione dei fornitori	Processo di Gestione dei fornitori	Descrizione formale del processo di gestione dei fornitori.
		Underpinning Contract	Accordo formale tra l'organizzazione IT ed il fornitore, descrivendo i ruoli e le responsabilità di entrambe le parti e obiettivi che devono essere raggiunti.

Livello 1	Livello 2	Controllo	Descrizione
Processi di risoluzione	Gestione dell'incidente e della richiesta di servizio	Processo di Gestione degli incidenti	Descrizione formale del processo di gestione degli incidenti.
		Catalogo degli Incidenti	Deve essere presente un catalogo che documenta le varie categorie di incidente al fine di classificarli ed ottenere una gestione efficiente degli incidenti.
		Record degli Incidenti	Record contenente tutte le informazioni necessarie per la valutazione degli incidenti, diagnosi, recupero e risoluzione.
		Report dei maggiori incidenti	Documento con tutti i dettagli e le lezioni apprese dopo che ha avuto luogo un l'incidente maggiore.
	Gestione del problema	Processo di gestione dei problemi	Descrizione formale del processo di gestione dei problemi.
		Catalogo dei problemi	Deve essere presente un catalogo che documenta le varie categorie di problemi e serve per la risoluzione dei problemi nonché per la loro gestione.
		Problem Records	Record contenente tutte le informazioni necessarie per la valutazione del problema, diagnosi, recupero e risoluzione.
Processi di controllo	Gestione della configurazione	Processo di gestione della configurazione	Descrizione formale del processo di gestione della configurazione.
		Configuration Records	Record con tutti i dati rilevanti sulla configurazione degli items al fine di mantenere il controllo della gestione dei servizi.
		Piano di gestione della configurazione	Un documento che definisce tutte le regole, l'ambito e responsabilità per implementare il servizio e Gestione della configurazione all'interno dell'organizzazione.
	Gestione del cambiamento	Processo di gestione del cambiamento	Descrizione formale del processo di gestione del cambiamento.
		Politiche di gestione del cambiamento	Linea guida per il processo, definire tutti gli aspetti importanti del Processo di gestione del cambiamento.
		Request for Change	Documento formale che descrive la modifica richiesta e avvia le attività di gestione delle modifiche.
		Change Record	Record contenente tutte le informazioni necessarie per la valutazione del cambiamento, approvazione e implementazione.

Livello 1	Livello 2	Controllo	Descrizione
Processi di controllo	Gestione del rilascio e messa in funzione	Processo di rilascio e messa in funzione	Descrizione formale del processo di rilascio e messa in funzione.
		Piano di rilascio e messa in esercizio	Un piano formale su come eseguire il rilascio e implementazione del servizio.
		Processo di Validazione e Testing	Descrizione formale del processo di Validazione e Testing.
		Test Plan	Documenta che pianifica e registra i test sui servizi ed i relativi risultati.
		Processo di gestione della conoscenza	Descrizione formale del processo di gestione della conoscenza.
		Piano di gestione della conoscenza	Un documento con lo scopo di definire e gestire le fonti di conoscenza che l'organizzazione usa. Definisce la tecnologia supporta da tale conoscenza e l'uso della conoscenza stessa.

2. Procedure attese delle PA vs ISO 22301

Livello 1	Livello 2	Controllo	Descrizione
Contesto dell'organizzazione	Comprendere le esigenze e le aspettative delle parti interessate	Requisiti legali e regolamentari	Procedure per l'identificazione dei requisiti legali e regolamentari applicabili.
			Lista delle prescrizioni legali, regolamenti ed altri requisiti.
	Determinare il campo di applicazione del sistema di gestione per la continuità operativa	Campo di applicabilità del BCMS	Documentazione riportante i confini, applicabilità del BCMS (Business Continuity Management System) e campo di applicazione.
		Esclusioni definite	Documentazione con le giustificazioni alle esclusioni.
Leadership	Impegno della direzione	Leadership e impegni dell'alta direzione	Definizione della politica per la continuità operativa.
			Lista degli obiettivi e piani per la BCMS.
			Documento contenente i ruoli, responsabilità e competenze per la gestione della continuità operativa.

Livello 1	Livello 2	Controllo	Descrizione
Attività operative	Analisi di impatto sul business e valutazione dei rischi	BIA	Processo per l'analisi dell'impatto (BIA) e valutazione dei rischi.
		Risultati della BIA	Documenti contenente i risultati della BIA.
		Valutazione dei rischio	Risultati della valutazione dei rischi.
		RTO	Determinazione dei valori di RTO.
		RPO	Determinazione dei valori di RPO.
		Determinazione e scelta della strategia	Valutazione delle capacità di continuità operativa dei fornitori.
		Risorse necessarie	Devono essere stabilite le risorse necessarie per attuare le strategie selezionate.
		Protezione e mitigazione	Definire il trattamento del rischio sulla base della propensione al rischio.
	Stabilire e attuare le procedure per la continuità operativa	Procedure di continuità operativa	Documento contenente le procedure di continuità operativa
		Struttura per la reazione agli incidenti	Procedure per la reazione agli incidenti
	Piani per la continuità operativa	Piani di continuità operativa	Procedure per rispondere alle interruzioni dell'attività
		Recupero e ripristino	Procedure per definire come continuare o recuperare le proprie attività entro un intervallo temporale predefinito. Procedure per il ripristino ed il ritorno delle attività operative attraverso delle misure temporanee adottate per supportare i normali requisiti di operatività dopo un incidente.
Valutazione delle prestazioni	Monitoraggio, misurazione, analisi e valutazione	Monitoraggio, misurazione, analisi e valutazione	Procedure per il monitoraggio delle prestazioni.

3. Procedure attese delle PA vs ISO 27001

Livello 1	Livello 2	Controllo	Descrizione
Processi per l'erogazione del servizio	Indirizzi della direzione per la sicurezza delle informazioni	Politiche per la sicurezza delle informazioni	Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti.
Organizzazione della sicurezza delle informazioni	Organizzazione interna	Ruoli e responsabilità per la sicurezza delle informazioni	Tutte le responsabilità relative alla sicurezza delle informazioni devono essere definite e assegnate.
Sicurezza delle risorse umane	Durante l'impiego	Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni	Tutto il personale dell'organizzazione e, quando pertinente, i collaboratori, devono ricevere un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa.
Gestione degli asset	Classificazione delle informazioni	Etichettatura delle informazioni	Deve essere sviluppato e attuato un appropriato insieme di procedure per l'etichettatura delle informazioni in base allo schema di classificazione adottato dall'organizzazione.
		Trattamento degli asset	Deve essere sviluppato e attuato un insieme di procedure per il trattamento degli asset in base allo schema di classificazione adottato dall'organizzazione.
Controllo degli accessi	Requisiti di business per il controllo degli accessi	Politica di controllo degli accessi	Una politica di controllo degli accessi deve essere definita, documentata ed aggiornata sulla base dei requisiti di business e di sicurezza delle informazioni.
	Gestione degli accessi degli utenti	Registrazione e deregistrazione degli utenti	Deve essere attuato un processo formale di registrazione e de- registrazione per abilitare l'assegnazione dei diritti di accesso.
		Provisioning degli accessi degli utenti	Deve essere attuato un processo formale per l'assegnazione o la revoca dei diritti di accesso per tutte le tipologie di utenze e per tutti i sistemi e servizi.
	Controllo degli accessi ai sistemi e alle applicazioni	Limitazione dell'accesso alle informazioni	Accesso a informazioni e funzioni di sistemi applicativi deve essere limitato secondo le politiche di controllo degli accessi.
		Procedure di log-on sicure	Quando richiesto dalle politiche di controllo degli accessi, l'accesso a sistemi e applicazioni deve essere controllato da procedure di log-on sicure.

Livello 1	Livello 2	Controllo	Descrizione
Sicurezza fisica e ambientale	Aree Sicure	Perimetro di sicurezza fisica	Si devono definire e usare dei perimetri di sicurezza per proteggere le aree che contengono informazioni critiche e le strutture di elaborazione delle informazioni.
		Controlli di accesso fisico	Le aree di sicurezza devono essere protette da appropriati controlli per l'ingresso atti ad assicurare che solo il personale autorizzato abbia il permesso di accedervi.
		Rendere sicuri uffici, locali e strutture	Deve essere progettata e applicata la sicurezza fisica agli uffici, ai locali ed agii impianti.
		Protezione contro minacce esterne ed ambientali	Deve essere progettata e applicata un'adeguata protezione fisica da calamità naturali, attacchi malevoli o accidenti.
		Lavoro in aree sicure	Devono essere progettate e attuate procedure per lavorare nelle aree sicure.
	Apparecchiature	Disposizione delle apparecchiature e loro protezione	Le apparecchiature devono essere disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato.
		Infrastrutture di supporto	Le apparecchiature devono essere protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari.
		Sicurezza dei cablaggi	I cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informativi devono essere protetti da intercettazioni, interferenze o danneggiamenti.
		Manutenzione delle apparecchiature	Le apparecchiature devono essere correttamente mantenute per assicurare la loro continua disponibilità e integrità.
		Sicurezza delle apparecchiature e degli asset all'esterno delle sedi	Devono essere previste misure di sicurezza per gli asset all'esterno delle sedi dell'organizzazione, considerando i diversi rischi derivanti dall'operare all'esterno dei locali dell'organizzazione stessa.

Livello 1	Livello 2	Controllo	Descrizione
Sicurezza delle attività operative	Procedure operative e responsabilità	Procedure operative documentate	Devono essere documentate e rese disponibili delle procedure operative a tutti gli utenti che le necessitano.
		Gestione dei cambiamenti (sistemistici)	I cambiamenti all'organizzazione, ai processi di business, alle strutture di elaborazione delle informazioni e ai sistemi che potrebbero influenzare la sicurezza delle informazioni devono essere controllati.
	Backup	Backup delle informazioni	Le apparecchiature devono essere disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato.
	Raccolta di log e monitoraggio	Raccolta di log degli eventi (e monitoraggio)	La registrazione dei log degli eventi, delle attività degli utenti, delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni deve essere effettuata, mantenuta e riesaminata periodicamente.
		Log di amministratori e operatori	Le attività degli amministratori e degli operatori di sistema devono essere sottoposte a log, e questi devono essere protetti e riesaminati periodicamente.
	Gestione delle vulnerabilità tecniche	Gestione delle vulnerabilità tecniche	Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere valutata e appropriate misure devono essere intraprese per affrontare i rischi relativi.
Sicurezza delle comunicazioni	Gestione della sicurezza della rete	Controlli di rete	Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni.
	Trasferimento delle informazioni	Politiche e procedure per il trasferimento delle informazioni	Devono esistere politiche, procedure e controlli formali a protezione del trasferimento delle informazioni attraverso l'uso di tutte le tipologie di strutture di comunicazione.
Acquisizione, sviluppo e manutenzione dei sistemi	Sicurezza nei processi di sviluppo e supporto	Politica per lo sviluppo sicuro	Le regole per lo sviluppo del software e dei sistemi devono essere stabilite ed applicate agli sviluppi all'interno dell'organizzazione.

Livello 1	Livello 2	Controllo	Descrizione
Relazioni con i fornitori	Sicurezza delle informazioni nelle relazioni con i fornitori	Politica per la sicurezza delle informazioni nei rapporti con i fornitori	I requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso agli asset dell'organizzazione da parte dei fornitori devono essere concordati con i fornitori stessi e documentati.
		Indirizzare la sicurezza all'interno degli accordi con i fornitori	Tutti i requisiti relativi alla sicurezza delle informazioni devono essere stabiliti e concordati con ciascun fornitore che potrebbe avere accesso, elaborare, archiviare, trasmettere o fornire componenti dell'infrastruttura IT per le informazioni dell'organizzazione.
		Filiera di fornitura per l'ICT (Information and communication technology)	Gli accordi con i fornitori devono includere i requisiti per affrontare i rischi relativi alla sicurezza delle informazioni associati ai servizi e ai prodotti della filiera di fornitura per l'ICT.
Gestione degli incidenti relativi alla sicurezza delle informazioni	Gestione degli incidenti relativi alla sicurezza delle informazioni e dei miglioramenti	Gestione degli incidenti: Responsabilità e procedure	Devono essere stabilite le responsabilità e le procedure di gestione per assicurare una risposta rapida, efficace ed ordinata agli incidenti relativi alla sicurezza delle informazioni.
		Segnalazione degli eventi relativi alla sicurezza delle informazioni	Gli eventi relativi alla sicurezza delle informazioni devono essere segnalati il più velocemente possibile attraverso appropriati canali gestionali.
		Raccolta di evidenze	L'organizzazione deve definire ed applicare opportune procedure per l'identificazione, la raccolta, l'acquisizione e la conservazione delle informazioni che possono essere impiegate come evidenze.
Conformità	Conformità ai requisiti cogenti e contrattuali	Identificazione della legislazione applicabile e dei requisiti contrattuali	Per ogni sistema informativo e per l'organizzazione in generate si devono esplicitamente definire, documentare e mantenere aggiornati tutti i requisiti cogenti e contrattuali pertinenti, oltre all'approccio stesso dell'organizzazione per soddisfarli.
		Diritti di proprietà intellettuale	Devono essere attuate delle procedure adeguate a garantire la conformità ai requisiti cogenti e contrattuali per l'uso del materiale sul quale potrebbero insistere diritti di proprietà intellettuale e per l'uso di prodotti software proprietari.

Livello 1	Livello 2	Controllo	Descrizione
Conformità	Conformità ai requisiti cogenti e contrattuali	Protezione delle registrazioni	Le registrazioni devono essere protette da perdita, distruzione, falsificazione, accesso non autorizzato e rilascio non autorizzato in conformità ai requisiti cogenti, contrattuali e di business.
		Privacy e protezione dei dati personali	Si devono assicurare la privacy e la protezione dei dati personali, come richiesto dalla legislazione e dai regolamenti pertinenti, per quanto applicabile.
		Regolamentazione sui controlli crittografici	I controlli crittografici devono essere utilizzati in conformità a tutti gli accordi, la legislazione e i regolamenti pertinenti.
	Riesami della sicurezza delle informazioni	Riesame indipendente della sicurezza delle informazioni	L'approccio dell'organizzazione alla gestione della sicurezza delle informazioni e la sua attuazione (ossia, gli obiettivi di controllo, i controlli, le politiche, i processi e le procedure per la sicurezza delle informazioni) devono essere riesaminati in modo indipendente ad intervalli pianificati oppure quando si verificano cambiamenti significativi.