CITTÀ SICURE DIGITALI

CSD8

PROFESSIONALE

GIOVANNA **PANUCCI** STEFANO **MANZELLI**

GIUSEPPE **ALVERONE**

COMPLIANCE PRIVACY

Percorsi per imprese e p.a.

#TECH
#LEGAL
#ESG

CITTÀ SICURE DIGITALI

CSD

EDIZIONI SIMONE PROFESSIONALE

CHECK LIST PER BCP e BIA (per verificare i suggerimenti forniti nel Capitolo 4 della Parte Seconda)

Le seguenti check list, pur essendo essenziali e basilari, possono aiutare a verificare se il Piano di Continuità Operativa/Aziendale (BCP) e la connessa Analisi di Impatto Aziendale (BIA) siano state sviluppate secondo i criteri suggeriti nella Guida Operativa.

##	Check Point per BCP	SI	NO	NA
	Identificazione delle MCA (Mission Critical Activities)			
1.BCP	Sono state individuate le attività essenziali (MCA) senza le quali l'organizzazione non può raggiungere i propri obiettivi di business?			
2.BCP	Sono state classificate le MCA in base alla loro importanza per gli obiettivi di business?			
	Identificazione degli Asset di Supporto			
3.BCP	Sono stati individuati gli asset di supporto (infrastrutture, personale, impianti, componenti tecnologiche, ecc.) per ciascuna MCA?			
4.BCP	Sono state identificate le interdipendenze tra gli asset di supporto e le MCA?			
	Analisi dei Rischi			
5.BCP	Sono stati individuati i fattori di rischio per le MCA e i relativi asset di supporto?			
6.BCP	È stata valutata la probabilità di occorrenza delle minacce e l'impatto potenziale sulla riservatezza, integrità, e disponibilità dei dati e delle informazioni?			
7.BCP	Sono state valutate le conseguenze in termini di limitazione dell'operatività?			

##	Check Point per BCP	SI	NO	NA
	Misure di Mitigazione			
8.BCP	Sono state individuate le misure di mitigazione che possono essere implementate per trattare i rischi identificati?			
9.BCP	Sono state coinvolte tutte le parti rilevanti nell'identificazione e implementazione delle misure di mitigazione?			
	CRevisione e Aggiornamento del BCP			
10.BCP	È prevista una revisione periodica del BCP per assicurarsi che rimanga aggiornato ed efficace di fronte ai cambiamenti organizzativi o tecnologici?			
	Test, formazione ed esercitazioni del BCP			
11.BCP	Sono pianificati test regolari, formazione ed esercitazioni per verificare l'efficacia del BCP e identificare eventuali aree di miglioramento?			
12.BCP	Viene documentato l'esito di test, formazione ed esercitazioni?			
13.BCP	È prevista l'implementazione di azioni correttive basate sulle lezioni apprese?			
	Procedure di comunicazione			
14.BCP	Sono definite procedure per le comunicazioni interne ed esterne in caso di interruzione?			
15.BCP	È stata designata l'autorità per le comunicazioni di emergenza?			
16.BCP	Sono state incluse procedure per la diffusione di rapporti sullo stato dell'incidente e per comunicati stampa?			
	Piano di ripristino di emergenza (DRP)			
17.BCP	È definito il modo in cui il DRP supporta il BCP nel recuperare i sistemi di supporto per le MCA in una sede alternativa?			
18.BCP	Sono stabilite le specifiche del DRP per le interruzioni del sistema informativo che richiedono il trasferimento?			

##	Check Point per BIA	SI	NO	NA
	Conseguenze dell'interruzione			
1.BIA	È stato valutato quali sarebbero le conseguenze di un'interruzione delle MCA e/o della disponibilità degli asset di supporto?			
2.BIA	È stato valutato come ciò influenzerebbe ciò i servizi forniti e i processi aziendali critici?			
	Tempi di inattività accettabili e perdite di dati sostenibili			
3.BIA	Sono stati definiti i tempi di inattività accettabili per ciascuna MCA e asset di supporto in caso di interruzione?			
4.BIA	Sono stati definiti i livelli di perdita di dati possono essere tollerati?			
5.BIA	Sono stati definiti i livelli minimi di operatività che devono essere mantenuti?			

##	Check Point per BIA	SI	NO	NA
	Coinvolgimento dell'Alta Direzione e dei Process Owner			
6.BIA	L'Alta Direzione, i responsabili delle diverse funzioni aziendali e i Process Owner sono stati coinvolti nell'analisi delle MCA e nella determinazione dei tempi di inattività accettabili e delle perdite di dati sostenibili?			
	Comprensione e Definizione dei Parametri			
7.BIA	È stato definito il tempo massimo di inattività tollerabile per ciascuna funzione aziendale critica prima che l'organizzazione subisca impatti inaccettabili: MTDT (Maximum Tolerance Down Time)?			
8.BIA	È stata definita la quantità massima di dati che ciascuna funzione aziendale critica può permettersi di perdere senza subire impatti significativi: MTDL (Maximum Tolerance Data Loss)?			
9.BIA	È stato definito l'obiettivo di tempo massimo per il ripristino della disponibilità di risorse o asset critici dopo un'interruzione: RPO (Recovery Point Objective)?			
10.BIA	È stato definito l'obiettivo di tempo massimo per il ripristino della disponibilità di risorse o asset critici dopo un'interruzione: RTO (Recovery Time Objective)?			
11.BIA	È stata fatta un'analisi costo-beneficio delle soluzioni di ripristino proposte per garantire che gli RTO siano mantenuti entro i limiti dell'MTDT?			
12.BIA	È stato definito il punto nel tempo (momento specifico prima dell'interruzione) fino al quale i dati devono essere ripristinati per minimizzare la perdita di dati: RPO (Recovery Point Objective)?			
13.BIA	È stato definito il livello minimo di operatività che l'organizzazione deve sostenere per raggiungere i propri obiettivi di business dopo un incidente: MBCO (Minimum Business Continuity Objective)?			
	Backup e Ripristino dei Dati			
14.BIA	Sono state stabilite procedure efficaci per il backup e il ripristino dei dati che rispettano l'RPO per ogni funzione aziendale critica?			
15.BIA	È stata definita una politica di sicurezza e di integrità dei dati?			
16.BIA	Sono state adottate misure per proteggere i dati da accessi o utilizzi non autorizzati?			
17.BIA	Viene gestita la crittografia dei dati, sia per i dispositivi di archiviazione primari che per i supporti di backup?			
	Sito Alternativo e Asset			
18.BIA	È stato identificato un sito alternativo adeguato a soddisfare gli obiettivi di ripristino dei sistemi?			
19.BIA	Sono stati catalogati tutti gli asset presenti nel sito alternativo e le loro funzioni?			

##	Check Point per BIA	SI	NO	NA
	Personale e Ruoli			
20.BIA	Quali sono i livelli minimi di personale necessari per mantenere la continuità operativa?			
21.BIA	Sono stati assegnati ruoli e responsabilità specifici al personale individuato?			