Transizione Digitale

Regolamento Cloud - checklist livelli minimi servizi ORDINARI

https://www.transizionedigitale.it/

Sezione	Sottosezione	Requisito	Codice	Descrizione		Stato di Adeguamento
2.1 Affidabilità	2.1.1) Alta Affidabilità	A.AA-01: Disponibilità dell'infrastruttura	1_O. L'indice di disponibilità dell'Infrastruttura Digitale, riferita alla percentuale di tempo in un anno in cui l'infrastruttura risulta essere accessibile e usabile, deve essere stato almeno pari:	a. 99,98% al netto dei fermi programmati;		
				b. 99,6 % comprendendo i fermi programmati.		
		A.AA-02: Sono disponibili soluzioni per la configurazione dei servizi in alta affidabilità	1_O. Il Centro di elaborazione dati (CED) deve essere dotato di soluzioni hardware e software (apparati di rete e sicurezza, storage, servizi di virtualizzazione, etc.) per la configurazione dei servizi in alta affidabilità. Devono essere inoltre messe a disposizione capability e funzionalità a supporto di configurazioni dei servizi in alta affidabilità quali:	a. Scelta della replica locale dei dati per un servizio storage;		
				b. Presenza di servizi di bilanciamento di carico;		
				c. Meccanismi di anti-affinity per la distribuzione delle istanze computazionali.		
	2.1.2) Business Continuity e Disaster Recovery	A.BC-01: Sono disponibili soluzioni di Disaster Recovery con tempi di ripristino garantiti	1_O. Provider di infrastruttura: L'infrastruttura digitale è dotata di soluzioni di DR, con caratteristiche coerenti con l'analisi del rischio, e deve garantire tempi di ripristino (RTO e RPO) variabili in funzione della criticità dell'applicazione ospitata conformemente con quanto definito nella BIA.			
			2_O. Con riferimento ai valori di RTO e RPO definiti al punto 1_O, devono comunque essere garantiti almeno i seguenti parametri di ripristino in caso di disastro: RTO 48 ore e RPO 48 ore.			
	2.1.3) Governance e processi	A.GP-01: I Servizi IT sono gestiti conformemente agli standard di settore	1_O. Sono adottati processi e procedure in linea con le best practice indicate dalla ISO/IEC 20000-2.			
		A.GP-02: È garantito il rispetto degli indicatori di servizio obbligatori	1_O. Per il Centro di elaborazione dati (CED), il soggetto deve garantire il supporto tecnico per emergenze con:	a. una copertura di 24 ore al giorno, 7 giorni a settimana per tutto l'anno;		
				b. un tempo massimo di risposta agli incidenti (inteso come tempo massimo che intercorre tra la segnalazione di un evento con impatto critico sull'operatività dell'Amministrazione e la risposta da parte del soggetto) pari a 1 ora.		
			2_O. Il soggetto deve garantire, per i servizi del Centro di elaborazione dati (CED) offerti, un supporto tecnico con le seguenti caratteristiche:	a. fornito, almeno in lingua inglese, dalle 08.00 alle 18.00 (ora italiana) nei giorni lavorativi		
				b. accessibile preferenzialmente tramite i seguenti canali: recapito telefonico ed e-mail. Su richiesta dell'Amministrazione, il servizio di supporto è fornito almeno in lingua italiana.		
	2.1.4) Performance e Scalabilità	A.PS-01: Sono garantite caratteristiche minime di connettività	1_O. Il soggetto deve fornire connettività su rete pubblica e rete privata. La rete privata deve consentire al soggetto di fruire di servizi di connettività dedicati e con le seguenti prestazioni minime garantite:	a. bandwidth di base 500 Mbps, con possibilità di incrementare la banda fino a 10 Gbps.		
2.2 Capacità Elaborativa	2.2.1) Capacità Elaborativa	CE.CE-01: Gestione della capacità di elaborazione conformemente agli standard o le best practice di settore	1_O. La capacità elaborativa dell'Infrastruttura Digitale è gestita attraverso un processo formale aderente alle best practice sul capacity management ITIL o alle linee guida presenti alla ISO/IEC 20000-2.			
2.3 Data Center Security	2.3.1) Data Center Security	S.DC-01: I Centri di elaborazione dati (CED) rispettano livelli minimi di sicurezza fisica e infrastrutturale	1_O. Il soggetto garantisce il presidio operativo all'interno del Data Center per 24 ore al giorno, 7 giorni a settimana per tutto l'anno.			
			2_O. Il Data Center è stato progettato e realizzato secondo standard di riferimento infrastrutturali, ad esempio ANSI/BICSI 002, TIA-942, EN 50600, Uptime Institute Tier Certification o analoghi.			
			3_O. Il soggetto garantisce le caratteristiche antincendio del Data Center in conformità alle norme antincendio vigenti.			
			4_O. Nei locali ospitanti i Data Center sono presenti pavimenti flottanti qualora la distribuzione dell'alimentazione elettrica e del cablaggio non avvenga per via aerea.			

Transizione Digitale

Regolamento Cloud - checklist livelli minimi servizi ORDINARI

https://www.transizionedigitale.it/

Sezione	Sottosezione	Requisito	Codice	Descrizione		Stato di Adeguamento
			5_O. Il soggetto garantisce che tutti i server dei Data Center sono connessi ad apparati per la continuità elettrica (UPS).			
		S.DC-02: Sono adottate misure di sicurezza fisica e ambientale	1_O. Esiste un documento di dettaglio che definisce politiche e procedure inerenti allo spostamento sicuro di supporti fisici. Queste policy e procedure dovranno essere riviste su base almeno annuale.			
			2_O. Sono implementati, manutenuti e adottati sistemi di sorveglianza all'esterno dei data center e in tutti i punti di ingresso e uscita al fine di rilevare ogni tentativo di ingresso non autorizzato.			
			3_O. Sono implementati, mantenuti e adottati, all'interno dei Data Center, i sistemi di controllo ambientale al fine di monitorare e testare l'adeguatezza delle temperature e le condizioni di umidità all'interno dell'area, nel rispetto dei principali standard di settore.			
2.4 Risparmio Energetico	2.4.1) Risparmio Energetico	RE.GE-01: Gestione energetica condotta in aderenza agli standard di settore	1_O. Il soggetto ha formalmente adottato procedure per la gestione delle emissioni dei gas prodotti, o per la gestione dell'energia consumata o per la gestione ambientale dei propri Data Center. A tale riguardo, il soggetto può fare riferimento, rispettivamente, agli standard ISO 14064, ISO 50001 e ISO 14001, o equivalenti.			
		RE.GE-02: Valutazione annuale dell'efficienza energetica del Data Center	1_O. Il soggetto determina con frequenza annuale l'efficienza energetica dei propri Data Center, ricorrendo al calcolo dell'indicatore Power Usage Effectiveness (PUE), che deve assumere valore massimo pari a 1,5. Il PUE mette in relazione la spesa energetica dell'infrastruttura, compresa di apparati IT, impianto di climatizzazione e impianti ausiliari, con la spesa esclusivamente riferita agli apparati IT. Nello specifico, è calcolato come il rapporto tra la spesa energetica sostenuta per tutta l'infrastruttura dei Data Center e quella sostenuta per gli apparati IT.			
2.5 Sicurezza	IDENTIFY (ID)	2.5.1) Asset Management (ID.AM): I dati, il personale, i dispositivi e i sistemi e le facilities necessari all'organizzazione sono identificati e gestiti in coerenza con gli obiettivi e con la strategia di rischio dell'organizzazione.	ID.AM-01: Sono censiti i sistemi e gli apparati fisici in uso nell'organizzazione	1_O. Tutti i sistemi e gli apparati fisici sono censiti ed esiste un elenco di quelli approvati da attori interni al soggetto.		
				2_O. Tutti i sistemi e gli apparati fisici presenti sulle reti sono censiti e l'accesso alla rete è consentito esclusivamente a quelli approvati.		
			ID.AM-03: I flussi di dati e comunicazioni inerenti l'organizzazione sono identificati	1_O. Tutti i flussi di dati e di informazioni, inclusi quelli verso l'esterno e relativi all'infrastruttura digitale, sono identificati, censiti e approvati da attori interni al soggetto.		
			ID.AM-06: Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)	1_O. È definita e resa nota alle articolazioni competenti del soggetto l'organizzazione di cybersecurity, anche con riferimento ai ruoli e alle responsabilità, per tutto il personale e per eventuali terze parti.		
				2_O. È nominato, nell'ambito dell'articolazione di cui al punto 1_O., un incaricato, e un eventuale sostituto, con il compito di gestire l'attuazione delle disposizioni del Regolamento in possesso di specifiche professionalità e competenze nella materia della sicurezza cibernetica, che riferisce direttamente al vertice gerarchico del soggetto ed assicura l'efficace implementazione delle misure di sicurezza di cui al presente Allegato.		

Sezione	Sottosezione	Requisito	Codice	Descrizione		Stato di Adeguamento
				3_O. Sono nominati, nell'ambito dell'articolazione di cui al punto 1_O., un referente tecnico, e almeno un suo sostituto, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, per lo svolgimento delle funzioni di interlocuzione con il CSIRT Italia ai fini della gestione degli incidenti aventi impatto sull'Infrastruttura digitale.		
				4_O. L'incaricato di cui al punto 2_O. e il referente tecnico di cui al punto 3_O. operano in stretto raccordo.		
		2.5.2) Governance (ID.GV): Le politiche, le procedure e i processi per gestire e monitorare i requisiti dell'organizzazione (organizzativi, legali, relativi al rischio, ambientali) sono compresi e utilizzati nella gestione del rischio di cybersecurity.	ID.GV-01: È identificata e resa nota una policy di cybersecurity	1_O. Esiste un documento aggiornato che descrive le politiche, i processi e le procedure di cybersecurity.		
		2.5.3) Risk Assessment (ID.RA): L'impresa comprende il rischio di cybersecurity inerente all'operatività dell'organizzazione (incluse la mission, le funzioni, l'immagine o la reputazione), gli asset e gli individui.	ID.RA-01: Le vulnerabilità delle risorse (es. sistemi, locali, dispositivi) dell'organizzazione sono identificate e documentate	1_O. Esiste un piano aggiornato di verifica e test di sicurezza che descrive l'insieme delle attività finalizzate alla valutazione del livello di sicurezza cibernetica dell'Infrastruttura digitale e dell'efficacia delle misure di sicurezza tecniche e procedurali e che contiene, inoltre, la periodicità e le modalità di esecuzione.		
				2_O. Esistono procedure, da aggiornare almeno su base annuale, per la gestione dei rischi associati a variazioni nell'ambito di asset organizzativi, ivi incluse applicazioni, sistemi, infrastrutture, configurazioni, ecc., indipendentemente dal fatto che gli asset siano gestiti internamente o esternamente (cioè in outsourcing).		
			ID.RA-05: Le minacce, le vulnerabilità, le relative probabilità di accadimento e conseguenti impatti sono utilizzati per determinare il rischio	1_O. L'analisi del rischio è svolta in funzione delle minacce, delle vulnerabilità, delle relative probabilità di accadimento e dei conseguenti impatti derivanti dal loro sfruttamento alla luce delle minacce considerate.		
				2_O. L'analisi del rischio tiene conto delle dipendenze interne ed esterne dell'Infrastruttura digitale.		
				3_O. Dopo aver identificato tutti i fattori di rischio e averli analizzati viene effettuata una ponderazione per determinare il livello di rischio.		
	PROTECT (PR)	2.5.4) Identity Management, Authentication and Access Control (PR.AC): L'accesso agli asset fisici e logici ed alle relative risorse è limitato al personale, ai processi e ai dispositivi autorizzati, ed è gestito in maniera coerente con la valutazione del rischio di accesso non autorizzato alle attività ed alle transazioni autorizzate.	PR.AC-01: Le identità digitali e le credenziali di accesso per gli utenti, i dispositivi e i processi autorizzati sono amministrate, verificate, revocate e sottoposte ad audit di sicurezza	1_O.a Le credenziali di accesso sono individuali per il personale del soggetto e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.		
				1_O.b Le credenziali di accesso sono individuali per il personale del soggetto e per il personale esterno che ha accesso all'infrastruttura e rispettano il principio di segregazione delle funzioni. Le credenziali sono aggiornate con una cadenza proporzionata ai privilegi dell'utenza.		
				2_O. Esistono politiche e procedure per la gestione delle credenziali di cui al punto 1_O., le quali dovranno essere aggiornate almeno su base annuale e rese disponibili, per la consultazione, all'Amministrazione.		

Sezione	Sottosezione	Requisito	Codice	Descrizione		Stato di Adeguamento
				3_O. Sono definiti meccanismi di gestione, memorizzazione e revisione delle informazioni in materia di credenziali, identità di sistema e livello di accesso.		
				4_O. Le credenziali sono aggiornate tempestivamente e senza ingiustificato ritardo qualora vi siano variazioni dell'utenza (es. trasferimento di personale).		
				5_O. Le identità di sistema sono gestite impiegando certificati digitali o tecniche alternative che assicurano un livello equivalente di sicurezza.		
				6_O. Esiste una pianificazione aggiornata degli audit di sicurezza per verificare il rispetto di quanto previsto nei punti 1_O., 2_O., 3_O., 4_O. e 5_O. ed esiste un registro degli audit effettuati con la relativa documentazione.		
			PR.AC-02: L'accesso fisico alle risorse è protetto e amministrato	1_O. Con riferimento ai censimenti della sottocategoria ID.AM-01, esiste un documento aggiornato di dettaglio contenente almeno:	a. le politiche di sicurezza adottate per la protezione e l'amministrazione degli accessi fisici;	
					b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.	
				2_O. È definito un perimetro di sicurezza fisico al fine di salvaguardare il personale, i dati e i sistemi informativi.		
			PR.AC-03: L'accesso remoto alle risorse è amministrato	1_O. Gli accessi da remoto effettuati sono monitorati da parte dell'organizzazione di cybersecurity.		
				2_O. Fatti salvi documentati limiti tecnici, sono implementate adeguate misure di controllo dell'accesso, adottando sistemi di autenticazione, autorizzazione e registrazione/contabilizzazione centralizzata degli accessi, coadiuvati da sistemi di autenticazione, la cui sicurezza è proporzionale al rischio.		
				3_O. È definito e implementato un modello di gestione degli accessi centralizzato volto ai processi di autorizzazione, logging e comunicazione degli accessi alle risorse e ai dati dell'Amministrazione.		
				4_O. Esiste un log degli accessi eseguiti da remoto.		
				5_O. Per gli accessi da remoto, sono impiegati modalità di autenticazione a fattore multiplo.		
			PR.AC-04: I diritti di accesso alle risorse e le relative autorizzazioni sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni	1_O. Sono definite, con riferimento ai censimenti di cui alla categoria ID.AM, almeno:	a. le risorse censite a cui è necessario accedere, per quali funzioni e con quali autorizzazioni;	
					b. i gruppi di utenti e i loro privilegi in relazione alle risorse a cui possono accedere e con quali autorizzazioni;	
					c. l'assegnazione degli utenti censiti a gruppi di utenti.	

Sezione	Sottosezione	Requisito	Codice	Descrizione		Stato di Adeguamento
				2_O. Nell'ambito di implementazione dell'accesso al sistema informativo, vengono osservati principi di separazione delle funzioni e del privilegio minimo in relazione al rischio organizzativo.		
				3_O. Sono definite e implementate politiche, procedure e misure tecniche per la segregazione dei ruoli di accesso privilegiato in modo che l'accesso amministrativo ai dati, le capacità di crittografia e gestione delle chiavi e le capacità di registrazione siano distinte e separate.		
		2.5.5) Awareness and Training (PR.AT): Il personale e le terze parti sono sensibilizzate in materia di cybersecurity e vengono addestrate per adempiere ai loro compiti e ruoli coerentemente con le politiche, le procedure e gli accordi esistenti.	PR.AT-01: Il personale del soggetto è informato e addestrato	1_O. Esiste un documento aggiornato di dettaglio che indica i contenuti dell'addestramento e della formazione fornita al personale del soggetto e le modalità di verifica dell'acquisizione dei contenuti.		
				2_O. L'addestramento e la formazione di cui al punto 1_O. fornita agli utenti del soggetto, in relazione ai ruoli, prevede, almeno, le seguenti tematiche:	a. la tutela della confidenzialità di dati in chiaro o cifrati;	
					b. la restituzione dei beni di natura aziendale al termine del rapporto di lavoro;	
					c. la definizione di ruoli e delle responsabilità;	
					d. politiche di accesso a sistemi, asset e risorse;	
					e. politiche di gestione delle informazioni e della sicurezza;	
					f. processi di comunicazione di ruoli e responsabilità ai dipendenti che hanno accesso ad asset informativi;	
					g. requisiti per la non divulgazione/confidenzialità di informazioni.	
			PR.AT-02: Gli utenti con privilegi (es. Amministratori di Sistema) comprendono i loro ruoli e responsabilità	1_O. Sono definiti i contenuti dell'istruzione fornita al personale del soggetto con privilegi e le modalità di verifica dell'acquisizione dei contenuti.		
				2_O. Sono definiti, per ogni membro del personale del soggetto, i privilegi e le istruzioni ricevute.		
		2.5.6) Data Security (PR.DS): I dati sono memorizzati e gestiti in accordo alla strategia di gestione del rischio dell'organizzazione, al fine di garantire l'integrità, la confidenzialità e la disponibilità delle informazioni.	PR.DS-01: I dati memorizzati sono protetti	1_O. Esiste un documento aggiornato di dettaglio che indica, anche in relazione alla categoria ID.AM, almeno:	a. le politiche di sicurezza adottate per la memorizzazione e la protezione dei dati;	
					b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.	
				2_O. I dati dell'amministrazione, ivi inclusi quelli deputati alla sicurezza (quali, a titolo esemplificativo, i sistemi di controllo degli accessi), sono trattati mediante infrastrutture localizzate	a. Business Continuity e Disaster Recovery, anche se esternalizzate (ad esempio tramite cloud computing);	

Sezione	Sottosezione	Requisito	Codice	Descrizione		Stato di Adeguamento
				sul territorio dell'Unione europea. Salvo motivate e documentate ragioni di natura normativa o tecnica, nelle citate infrastrutture sono ricomprese quelle deputate alle funzioni di:	b. Content Delivery Network con distribuzione geografica globale. In tal caso, l'applicazione della misura ID. RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali.	
				3_O. Diversamente dal caso dei Metadata relativi al funzionamento dell'infrastruttura, che possono essere trattati mediante infrastrutture localizzate anche al di fuori del territorio dell'Unione europea, i Metadata relativi all'amministrazione sono trattati mediante infrastrutture localizzate sul territorio dell'Unione europea, salvo motivate e documentate ragioni di natura normativa o tecnica. In tal caso, l'applicazione della misura ID.RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali. In caso di trasferimento di Metadata verso infrastrutture extra-UE, l'interruzione di tale flusso di comunicazione non deve comportare comunque il mancato rispetto dei livelli minimi di servizio previsti per il servizio cloud.		
				4_O. Con riferimento al punto 3_O., nel caso in cui i Metadata relativi all'amministrazione siano finalizzati all'erogazione di servizi per la sicurezza informatica ovvero per la resilienza dell'infrastruttura digitale, essi possono essere trattati, in presenza di motivate ragioni tecniche e relative evidenze di una loro gestione conforme all'univocità delle finalità del trattamento, anche fuori del territorio europeo. In tal caso, l'applicazione della misura ID.RA-05 deve tenere opportunamente conto della localizzazione al di fuori del territorio europeo, verificando altresì la compliance rispetto alla normativa in tema di protezione dei dati personali. In caso di trasferimento di metadata verso infrastrutture extra-UE, l'interruzione di tale flusso di comunicazione non deve comportare comunque il mancato rispetto dei livelli minimi di servizio previsti per il servizio cloud.		
			PR.DS-05: Sono implementate tecniche di protezione (es. controllo di accesso) contro la sottrazione dei dati (data leak)	1_O. Sono definite in relazione alla categoria ID.AM, almeno:	a. le politiche di sicurezza adottate per l'accesso ai dati;	
					b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.	
				2_O. Sono adottate politiche di Data Loss Prevention coerentemente con la valutazione dei rischi.		

Transizione Digitale

Regolamento Cloud - checklist livelli minimi servizi ORDINARI

https://www.transizionedigitale.it/

Sezione	Sottosezione	Requisito	Codice	Descrizione		Stato di Adeguamento
			PR.DS-06: Sono impiegati meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni	1_O. Sono definiti in relazione alla categoria ID.AM, almeno:	a. l'elenco dei meccanismi di controllo dell'integrità dei dati per verificare l'autenticità di software, firmware e delle informazioni;	
					b. le politiche di sicurezza adottate per assegnare un meccanismo a una risorsa e quali di questi meccanismi è applicato a quale risorsa;	
					c. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.	
		2.5.7) Information Protection Processes and Procedures (PR.IP): Sono attuate e adeguate nel tempo politiche di sicurezza (che indirizzano, scopo, ambito, ruoli e responsabilità, impegno da parte del management e coordinamento tra le diverse entità organizzative), processi e procedure per gestire la protezione dei sistemi informativi e degli asset.	PR.IP-01: Sono definite e gestite delle pratiche di riferimento (c.d. baseline) per la configurazione dei sistemi IT e di controllo industriale che incorporano principi di sicurezza (es. principio di minima funzionalità)	1_O. Sono definite politiche e procedure con riferimento alla sicurezza delle applicazioni per fornire un adeguato supporto alla pianificazione, realizzazione e manutenzione delle funzionalità di sicurezza delle applicazioni, le quali dovranno essere riviste e aggiornate almeno su base annuale.		
			PR.IP-04: I backup delle informazioni sono eseguiti, amministrati e verificati	1_Oa. Viene effettuato periodicamente un backup dei dati memorizzati. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup.		
				1_Ob. Viene effettuato periodicamente un backup delle informazioni memorizzate nel cloud necessarie per il completo ripristino del sistema, ivi incluso i dati dell'Amministrazione e i dati necessari per il ripristino del servizio. Viene assicurata la riservatezza, l'integrità e la disponibilità dei dati dei backup. A tal fine, viene anche assicurato che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.		
				2_O. Viene verificato periodicamente il ripristino (test di restore) delle copie di backup come obiettivo (SLO) almeno 1 volta all'anno.		
			PR.IP-12: Viene sviluppato e implementato un piano di gestione delle vulnerabilità	1_O. Esiste un documento aggiornato di dettaglio che indica almeno:	a. le politiche di sicurezza adottate per gestire le vulnerabilità;	
					b. i processi, le metodologie e le tecnologie impiegate che concorrono al rispetto delle politiche di sicurezza.	
				2_O. Sono definite ed implementate procedure e misure tecniche volte all'aggiornamento degli strumenti di rilevamento, della threat signatures e degli indicatori di compromissione, le quali dovranno essere riviste e aggiornate frequentemente o su base settimanale.		
		2.5.8) Maintenance (PR.MA): La manutenzione dei sistemi informativi e di controllo industriale è fatta in accordo con le politiche e le procedure esistenti.	PR.MA-02: La manutenzione remota delle risorse e dei sistemi è approvata, documentata e svolta in modo da evitare accessi non autorizzati	1_O. La manutenzione delle risorse e dei sistemi (ivi incluse le attività relative alle funzioni di sicurezza) svolta da remoto è eseguita nel rispetto delle misure di cui alla sottocategoria PR. AC-03 e dei seguenti punti.		

Transizione Digitale

Regolamento Cloud - checklist livelli minimi servizi ORDINARI

https://www.transizionedigitale.it/

Sezione	Sottosezione	Requisito	Codice	Descrizione		Stato di Adeguamento
				2_O. Tutti gli accessi eseguiti da remoto da personale di terze parti sono autorizzati dall'organizzazione di cybersecurity e limitati ai soli casi essenziali.		
		2.5.9) Protective Technology (PR.PT): Le soluzioni tecniche di sicurezza sono gestite per assicurare sicurezza e resilienza di sistemi e asset, in coerenza con le relative politiche, procedure ed accordi.	PR.PT-04: Le reti di comunicazione e controllo sono protette	1_O. I sistemi perimetrali, quali firewall, anche a livello applicativo, sono presenti, aggiornati, manutenuti e ben configurati.		
	DETECT (DE)	2.5.10) Security Continuous Monitoring (DE.CM): I sistemi informativi e gli asset sono monitorati per indentificare eventi di cybersecurity e per verificare l'efficacia delle misure di protezione.	DE.CM-01: Viene svolto il monitoraggio della rete informatica per rilevare potenziali eventi di cybersecurity	1_O. Sono presenti sistemi di rilevamento delle intrusioni (Intrusion Detection Systems - IDS).		
				2_O. Sono presenti dei processi per il monitoraggio degli eventi relativi alla sicurezza delle applicazioni e dell'infrastruttura sottostante.		
			DE.CM-04: Il codice malevolo viene rilevato	1_O. Sono implementati ed utilizzati appositi strumenti per la prevenzione e il rilevamento di malware, nonché sistemi di protezione delle postazioni terminali (Endpoint Protection System - EPS).		
				2_O. Sono presenti politiche di protezione anti-malware, le quali dovranno essere riviste almeno su base annuale.		
			DE.CM-08: Vengono svolte scansioni per l'identificazione di vulnerabilità	1_O. In base all'analisi del rischio, sulle piattaforme e sulle applicazioni software ritenute critiche sono eseguiti penetration test e vulnerability assessment, prima della loro messa in esercizio.		
				2_O. Sono eseguiti periodicamente penetration test e vulnerability assessment in relazione alla criticità delle piattaforme e delle applicazioni software, di cui al punto 1_O.		
				3_O. Esiste un documento aggiornato recante la tipologia di penetration test e vulnerability assessment previsti.		
				4_O. Esiste un registro aggiornato dei penetration test e vulnerability assessment eseguiti corredato dalla relativa documentazione.		
		2.5.11) Detection Processes (DE.DP): Sono adottati, mantenuti e verificati processi e procedure di monitoraggio per assicurare la comprensione di eventi anomali.	DE.DP-01: Ruoli e responsabilità per i processi di monitoraggio sono ben definiti al fine di garantire l'accountability	1_O. Le nomine di cui alla sottocategoria ID.AM-06 sono rese note all'interno del soggetto.		
				2_O. I ruoli, i processi e le responsabilità per le attività propedeutiche al rilevamento di incidenti con impatto sull'Infrastruttura digitale sono ben definiti e resi noti alle articolazioni competenti del soggetto.		
	RESPOND (RS)	2.5.12) Communications (RS.CO): Le attività di risposta sono coordinate con le parti interne ed esterne (es. eventuale supporto da parte degli organi di legge o dalle forze dell'ordine).	RS.CO-01: Il personale conosce il proprio ruolo e le operazioni che deve svolgere in caso sia necessaria una risposta ad un incidente	1_O. I ruoli e le responsabilità per lo svolgimento delle fasi e dei processi di risposta ad un incidente sono ben definiti e resi noti alle articolazioni competenti del soggetto.		

Sezione	Sottosezione	Requisito	Codice	Descrizione		Stato di Adeguamento
		2.5.13) Analysis (RS.AN): Vengono condotte analisi per assicurare un'efficace risposta e supporto alle attività di ripristino.	RS.AN-05: Sono definiti processi per ricevere, analizzare e rispondere a informazioni inerenti vulnerabilità rese note da fonti interne o esterne all'organizzazione (es. test interni, bollettini di sicurezza, o ricercatori in sicurezza)	1_O. I canali di comunicazione del CSIRT Italia di cui all'articolo 4 del decreto del Presidente del Consiglio dei ministri 8 agosto 2019, dell'Autorità di riferimento del proprio settore produttivo, nonché di eventuali CERT e Information Sharing & Analysis Centre (ISAC) di riferimento sono monitorati.		
		2.5.14) Mitigation (RS.MI): Vengono eseguite azioni per prevenire l'espansione di un evento di sicurezza, per mitigare i suoi effetti e per risolvere l'incidente.	RS.MI-03: Le nuove vulnerabilità sono mitigate o documentate come rischio accettato	1_O. Le vulnerabilità sono mitigate secondo quanto previsto dal piano di gestione delle vulnerabilità (PR.IP-12), ovvero ne viene documentato e accettato il rischio residuo derivante dalla mancata mitigazione.		
				2_O. Sono definite ed implementate procedure e misure tecniche per consentire azioni di risposta (programmate o al sopraggiungere di emergenze) in caso di vulnerabilità identificate, in base al rischio.		
	RECOVER (RC)	2.5.15) Recovery Planning (RC.RP): I processi e le procedure di ripristino sono eseguite e mantenute per assicurare un recupero dei sistemi o asset coinvolti da un incidente di cybersecurity.	RC.RP-01: Esiste un piano di ripristino (recovery plan) e viene eseguito durante o dopo un incidente di cybersecurity	1_O. Esiste un piano di ripristino che prevede, almeno, i processi e le procedure necessarie al ripristino del normale funzionamento della porzione dell'infrastruttura coinvolta da un incidente di cybersecurity.		