ALLEGATO *B*

Misure di sicurezza applicate dalle SWH per lo svolgimento dei Servizi riguardanti i SW Gestionali impiegati nei contesti on premise e in cloud

Nel presente Allegato B sono individuate le misure di sicurezza da adottare per lo svolgimento dei Servizi nei contesti on premise e in cloud, tenuto conto dei diversi e specifichi rischi da fronteggiare in tali distinti contesti.

Per le misure di sicurezza sono stati confrontati, sempre se applicabili alle attività di cui sopra:

1. i controlli presenti nella "UNI CEI ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements" (ISO/IEC 27002:2022);

2. i controlli necessari per la "Privacy in base alla progettazione e privacy per impostazione predefinita" elencati nel paragrafo A.7.4 della "ISO/IEC 27701:2019 Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines" (ISO/IEC 27701:2019);

3. le misure comprese nelle "Misure minime di sicurezza ICT per le pubbliche amministrazioni" emanate dall'AgID (MM AgID);

4. le misure elencate riguardanti la "Sicurezza delle informazioni" presenti nel paragrafo 5.11 di " Information technology - Security techniques - Privacy framework" (ISO/IEC 29100:2011).

Le misure di sicurezza sono state confrontate con i parametri RID (riservatezza, integrità e disponibilità) utili per una valutazione degli impatti sugli interessati. Nella seconda sezione, le misure sono confrontate anche con il parametro Res (resilienza).

Misure di sicurezza applicate per lo svolgimento dei Servizi riguardanti i Software Gestionali impiegati nei contesti "on-premise"

Ambito	Catalogazione	Requisito di dettaglio	Riferimenti	RID
Gestione Account	Autorizzazione e autenticazione	Tutti gli operatori della SWH devono accedere alle piattaforme utilizzate per l'assistenza previa autenticazione con le credenziali nominative individuali. Nel caso di un tentativo d'accesso alla piattaforma di supporto con un account diverso da quello autorizzato, il sistema deve negare l'accesso. Le utenze degli operatori incaricati dell'assistenza sono periodicamente revisionate allo scopo di verificare che i permessi e le autorizzazioni di accesso siano sempre aggiornate.	ISO/IEC 27002:2022 5.3, 5.15, 5.16, 5.17, 5.18 MM AgID ABSC 5.6.1, 5.7, 5.8.1, 5.11 ISO/IEC 29100:2011 5.11	RID
	Assegnazione dei privilegi	L'assegnazione dei privilegi agli operatori deve avvenire in base al principio del "need-to-know" e della "segregation of duties".		
	Password policy	Le password di accesso degli operatori incaricati dell'assistenza devono essere composte da almeno dodici (12) caratteri, prevedere caratteri alfanumerici e caratteri speciali, essere sostituite almeno ogni novanta (90) giorni, qualora si tratti di utenze privilegiate nella configurazione del SW, e conservate in formato crittografato.		
	Utilizzo della VPN	L'erogazione del servizio di assistenza e di accesso alla piattaforma da remoto devono avvenire mediante connessione VPN con MFA. La VPN può essere del Cliente o configurata dalla SWH in accordo col Cliente; prima dell'utilizzo di ogni sessione ci deve essere l'autorizzazione del Cliente che deve attivare o disattivare l'accesso ai propri sistemi in relazione alle attività svolte e richieste dallo stesso. Al termine dell'intervento l'operatore di assistenza dovrà	ISO/IEC 27002:2022 8.21	RID

		comunicare al Cliente la fine dell'intervento e richiedere la disattivazione dell'accesso.		
Gestione Sicurezza Logica	Patch Management	Continuo patching applicativo di sicurezza relativo alla piattaforma per l'erogazione del supporto da remoto.	ISO/IEC 27002:2022 8.8	RID
Log Management	Monitoraggio e gestione dei log di attività	Le attività svolte dagli operatori con utenze privilegiate devono essere tracciate e monitorate.	ISO/IEC 27002:2022 8.15 MM AgID ABSC 5.4.1, 5.1.1	R
Supporto da remoto in modalità attended (con presidio di un soggetto autorizzato da parte del Cliente)	Gestione dell'escalation interna	Gli operatori incaricati dell'assistenza devono accertarsi che le richieste di assistenza provengano da un soggetto identificato e preventivamente autorizzato dal Cliente (ad esempio tramite autenticazione sulla piattaforma di ticketing).	ISO/IEC 27002:2022 5.16 ISO/IEC 29100:2011 5.11	RID
	Gestione del sistema di supporto	Gli operatori incaricati dell'assistenza devono richiedere al Cliente in modo tracciabile le autorizzazioni necessarie ai fini dell'erogazione del servizio di assistenza (ad esempio, la condivisione dello schermo, il controllo condiviso dell'applicativo, il trasferimento dei file e la registrazione delle attività).	NA	R
Supporto da remoto in modalità unattended	Assegnazione dei privilegi da parte del Cliente	Deve essere garantita al Cliente la possibilità di assegnare specifici diritti ai determinati operatori incaricati dell'assistenza al fine di limitare l'accesso ai propri sistemi solo al personale autorizzato e per un intervallo temporale definito.	ISO/IEC 27002:2022 5.15,5.16 ISO/IEC 29100:2011 5.11	R

Supporto da remoto in modalità unattended	Accesso al DB	L'accesso agli ambienti di produzione da parte di Utenti che non operano in qualità di amministratori di sistema è consentito unicamente in presenza di comprovate esigenze di assistenza/manutenzione e mediante un processo autorizzativo ad hoc che consenta di tracciare la richiesta/autorizzazione del Cliente (es. "trouble ticketing").	ISO/IEC 27002:2022 5.15,5.16, 5.17, 5.18 MM AgID ABSC 5.6.1, 5.7, 5.8.1, 5.11 ISO/IEC 29100:2011 5.11	RI
Attività di test	Utilizzo dei dati per l'esecuzione dei test	Utilizzo di dati fittizi (non dati reali) per l'esecuzione dei test. Solo in casi particolari, su richiesta del Cliente, ed in particolare quando sono sviluppate funzioni particolarmente complesse che devono essere provate e che devono essere verificate sull'esattezza della singola elaborazione e del singolo interessato presente negli archivi, prima di utilizzare gli archivi viene verificata l'adozione delle misure di sicurezza presenti negli ambienti di produzione. In questi casi i dati devono essere conservati per il tempo strettamente necessario all'esecuzione dell'attività di verifica della qualità e poi cancellati.	ISO/IEC 27002:2022 5.10	

	Accesso agli ambienti dei Clienti tramite IP pubblici	Il collegamento tramite IP pubblici su ambienti cloud dovrà avvenire da parte degli operatori incaricati dell'assistenza con utenze individuali, che dovranno essere attivate dal Cliente al fine di evadere la richiesta di assistenza. Solo nel caso in cui è previsto un servizio di assistenza continuativo tali credenziali potranno rimanere sempre attive, ma in questo caso gli accessi degli operatori dovranno essere loggati e l'operatore per ogni intervento dovrà giustificare la finalità per cui l'ha dovuto effettuare. Per tale finalità l'ambiente applicativo potrà prevedere utenze precaricate a sistema e le procedure di assegnazione delle stesse saranno in carico alla SWH in relazione alle esigenze segnalate dal Cliente.	ISO/IEC 27002:2022 5.15, 5.16, 5.17, 5.18 ISO/IEC 29100:2011 5.11	R
Gestione archivi	Autorizzazione per copia/trasferimento dati temporanei	L'eventuale copia o trasferimento di archivi o base dati del Cliente per finalità di assistenza o manutenzione deve essere preventivamente ed espressamente autorizzata dal Cliente stesso.	ISO/IEC 27002:2022 5.14	RI
	Secure disposal	I DB/archivi del Cliente devono essere conservati per il tempo strettamente necessario all'esecuzione dell'attività di assistenza e immediatamente cancellati qualora non più necessari per l'esecuzione delle operazioni di assistenza.	ISO/ISO 27701: A.7.4.6	R

		Le copie dei DB/archivi del Cliente prelevati per finalità di assistenza devono essere trasferite tramite canali sicuri e protetti, salvate in ambienti dotati delle opportune misure di sicurezza e non devono essere sottoposti a backup allo scopo di minimizzare il trattamento.	ISO/IEC 5.14, ISO/IEC A.7.4.9	27002:2022 8.26 27701:2019	R
	Secure disposal	Qualora durante le attività di assistenza fosse necessario stampare documenti o informazioni, tali documenti devono rimanere nell'esclusiva disponibilità dell'operatore e da questi devono essere protetti contro accessi non autorizzati. Al termine dell'attività, i documenti dovranno essere distrutti.	ISO/ISO 27701: A.7.4.6		R

	Attività di migrazione e conversione	In relazione alle attività di migrazione dei dati sono da prevedere le seguenti misure di sicurezza: - Utilizzo di canali sicuri e protetti nella trasmissione dei dati; - Utilizzo delle basi dati contenenti dati effettivi in ambiente dedicato, dotato di misure di sicurezza idonee a garantirne la riservatezza; - Configurazione dei profili di accesso a tali ambienti al solo personale preposto dalla SWH alla gestione delle attività di migrazione compreso il test ed il collaudo. Ove richiesto, tali profili sono estesi anche al personale del Cliente. Qualora presenti, gli accessi da remoto avvengono sempre mediante l'utilizzo di canali sicuri; - Conservazione dei dati esclusivamente fino al buon fine del completamento delle attività di verifica ed alla conseguente consegna, approvazione e accettazione da parte del Cliente.	ISO/IEC 5.14, 5.15, 27002:2022 8.26 ISO/IEC A.7.4.9 27701:2019	RI

Governance	Tracciabilità	Sono adottati processi e strumenti di assistenza che assicurino la tracciabilità degli interventi richiesti ed eseguiti (piattaforma di ticketing).	ISO/IEC 27002:2022 5.10	RID
Governance	Data Breach	Sono adottate procedure di gestione degli incidenti che consentono di individuare, contenere e risolvere situazioni di rischio (e.g. violazioni di dati personali) per la sicurezza dei dati e dei sistemi in fase post-intrusione.	ISO/IEC 27002:2022 5.5, 5.24, 5.25, 5.26, 5,27	RID

Misure di sicurezza applicate per lo svolgimento dei Servizi riguardanti i Software Gestionali impiegati nei contesti in cloud

Le misure che seguono devono essere applicate dalla SWH qualora il Software Gestionale sia utilizzato dal Cliente attraverso il Data Center della medesima SWH, oppure tramite Data Center esterni resi disponibili da sub-fornitori della SWH, di cui quest'ultima mantiene comunque la gestione amministrativa dei sistemi di erogazione della soluzione informatica. Qualora il servizio fosse erogato da Data center esterni che assumono anche la gestione sistemistica dei server e dell'infrastruttura necessari all'erogazione dei servizi, la SWH provvederà a vincolare il sub-fornitore al rispetto di misure di sicurezza a livello contrattuale e sottoporrà il DC esterno ad audit periodici per la verifica della relativa applicazione.

Ambito	**Catalogazione**	**Requisito di dettaglio**	**Riferimenti**	**RID Res**
Misure sicurezza Data Center	Accesso al Sistema o SW (autenticazione)	Adozione di misure dirette a garantire che: - gli accessi di amministrazione da parte della SWH siano riservati al personale a cui sia attribuita la qualifica ("ruolo") di amministratore di sistema, in virtù di elevate capacità tecniche e caratteristiche di comprovata affidabilità e moralità ; - l'accesso amministrativo ai sistemi da parte del personale del Cliente avverrà attraverso procedure di autenticazione a più fattori (MFA).	ISO/IEC 27002:2022 5.15, 5.16, 5.17, 5.18, 8.15 MM AgID ABSC 5.1.1, 5.4.1, 5.6.1, 5.7, 5.8.1, 5.11 ISO/IEC 29100:2011 5.11	RID

Misure sicurezza Data Center	Accesso al Sistema o SW (policy di gestione)	Per i servizi che prevedono una modalità di gestione amministrativa delle componenti infrastrutturali, devono essere previste le seguenti policy: - utenze che consentono l'individuazione dell'amministratore che esegue l'intervento; - attivazione di un processo di log management che identifichi i log in, log out e log in failed; - conservazione dei log in un formato che ne garantisca l'integrità e la lettura nel tempo; - conservazione dei log per almeno sei (6) mesi; - verifica annuale dell'operato degli amministratori di sistema; - accesso ai sistemi attraverso VPN e MFA.	ISO/IEC 27002:2022 5.3		
Misure sicurezza Data Center	Log Management	Funzionalità per il tracciamento o registrazione (log) degli accessi e delle attività svolte dagli Utenti. I log concernenti le attività svolte devono essere opportunamente protetti a garanzia della loro integrità e riservatezza. Tali funzionalità devono essere attivabili da parte dell'amministratore di sistema del Cliente o della Software House su richiesta del Cliente.	ISO/IEC 27002:2022 8.15	R	

Misure sicurezza Data Center	Auditing	Utilizzo del sistema di gestione e analisi dei log anche per il monitoraggio delle attività degli amministratori di sistema. L'accesso al sistema di gestione dei log è riservato al personale avente ruolo di auditor e non è ammesso per il personale addetto all'amministrazione di sistema.	ISO/IEC 27002:2022 8.16	R
Misure sicurezza Data Center	Crittografia dei protocolli di comunicazione	Applicazione di protocolli crittografici standard di comunicazione sicuri e non obsoleti, nei casi in cui l'accesso al sistema sia effettuato tramite Internet.	ISO/IEC 27002:2022 5.14, 8.21 ISO/IEC 29100:2011 5.11	RI
Misure sicurezza Data Center	Minacce e Vulnerabilità	Adozione di un programma di gestione delle minacce e dei rischi per monitorare continuamente le vulnerabilità delle Piattaforme SaaS indicate da best practice internazionali attraverso la pianificazione e l'esecuzione di scansioni delle vulnerabilità interne ed esterne e test di penetrazione. Le vulnerabilità identificate devono essere valutate per determinare i rischi associati e le opportune azioni correttive stabilite in base alla priorità assegnata e gravità rilevata.	ISO/IEC 27002:2022 8.8 MM AgID ABSC MM AgID ABSC 4.1.1, 4.1.2, 4.4.2, 4.6.1 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Firewalling	Adozione di sistemi di firewall finalizzati a filtrare e contenere il traffico identificando eventuale traffico anomalo indicatore di possibili attacchi informatici. Presenza di firewall L4 o L7/WAF.	ISO/IEC 27002:2022 5.14, 8.22 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Intrusion Prevention	Protezione dell'ambiente mediante cui è erogato il servizio dalla SWH mediante Intrusion Prevention System (IPS) che permettono di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso. Il traffico di rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito.	ISO/IEC 27002:2022 7.4, 8.21 ISO/IEC 29100:2011 5.11	RID Res

Misure sicurezza Data Center	Malware protection	Adozione di misure di protezione da infezioni di software malevolo, di difesa da azioni non autorizzate, da applicazioni sospette e di protezione da tentativi di sottrazione di dati personali (es. mediante sistemi antivirus, antispamming, antiphishing, etc., mantenuti costantemente aggiornati).	ISO/IEC 27002:2022 8.7 MM AgID ABSC 8 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Filesystem Antivirus	Adozione di moduli Antivirus sul filesystem su tutti i server utilizzati per la fornitura dei servizi, con possibilità di configurare, su base progettuale, prodotti antivirus specifici gestiti centralmente in termini di aggiornamento, distribuzione delle policy, avvio di scansioni on demand, notifiche e gestione della area di quarantena.	ISO/IEC 27002:2022 8.7 MM AgID ABSC 8 ISO/IEC 29100:2011 5.11	RD
Misure sicurezza Data Center	Monitoraggio e gestione incidenti	Adozione di policy e procedure per l'identificazione, gli interventi, i rimedi e le segnalazioni di incidenti che determinano un rischio per l'integrità o riservatezza dei dati personali o altre violazioni della sicurezza.	ISO/IEC 27002:2022 5.24, 5.25, 5.26, 5.27, 5.28, 6.8	RID Res
Misure sicurezza Data Center	Security Patch Management	Sottoposizione della piattaforma ad un processo periodico di verifica delle patch o delle fix disponibili relativamente alle componenti dell'impianto di erogazione e a quelle ritenute critiche per l'erogazione del servizio o per la sicurezza.	ISO/IEC 27002:2022 8.8 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Sicurezza fisica	Applicazione di adeguate misure di sicurezza fisica alla piattaforma hardware/software progettata (es. utilizzo di hosting providers/servizi di data center dotati di adeguati sistemi di prevenzione del rischio intrusione, incendio, allagamento, ecc.).	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11	ID Res

Misure sicurezza Data Center	Anti allagamento	Adozione nell'ambito del Data Center di tutte le misure necessarie a prevenire allagamenti (quali presenza di sonde, impianti di allarme, ecc.).	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11	ID Res
Misure sicurezza Data Center	Anti intrusione	Impostazione nel Data Center di un sistema di controllo degli accessi che identifichi coloro che accedono e impedisca l'accesso ai non autorizzati. La procedura deve prevedere anche la gestione del Change con l'attivazione e disattivazione dell'autorizzazione all'accesso in funzione dei cambi di ruolo.	ISO/IEC 27002:2022 7.1, 7.2 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Telecamere a circuito chiuso	Installazione di telecamere (CCTV) per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche.	ISO/IEC 27002:2022 7.4 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Condizionamento	Adozione di adeguati impianti di condizionamento e di raffreddamento degli ambienti ed apparati.	ISO/IEC 27002:2022 7.5, 7.8 ISO/IEC 29100:2011 5.11	ID Res
Misure sicurezza Data Center	Continuità ed emergenza	Adozione di procedure e controlli da eseguire al fine di garantire il necessario livello di continuità e disponibilità del sistema/SW (in caso di incidente / violazione di dati personali). Le procedure devono comprendere le indicazioni per la conservazione delle copie di backup nonché un piano per il disaster recovery.	ISO/IEC 27002:2022 5.4, 5.29 MM AgID ABSC 10 ISO/IEC 29100:2011 5.11	RID Res
Misure sicurezza Data Center	Cancellazione dei dati	Previsione di misure per la cancellazione dei dati di produzione al termine dell'erogazione del servizio secondo i termini contrattuali definiti con il Cliente.	ISO/IEC 27002:2022 8.10	R
Misure sicurezza Data center esterni	Verifica dei requisiti del sub-fornitore e contrattualizzazione degli obblighi relativi alle misure di sicurezza	Selezione e verifica dei requisiti del sub-fornitore che assume la gestione sistemistica dei server e dell'infrastruttura necessari allo svolgimento dei	ISO/IEC 27002:2022 5.19; 5.20	RID

		Servizi e sottoscrizione di un contratto che vincoli il medesimo sub-fornitore al rispetto degli obblighi concernenti le misure di sicurezza (previsti dalla SWH per la gestione del DC).		
Misure sicurezza Data center esterni	Audit nei confronti del sub-fornitore	Sottoposizione del sub-fornitore che gestisce il DC esterno ad audit periodici per la verifica del rispetto degli obblighi concernenti le misure di sicurezza, fatto salvo quanto previsto dalle condizioni di servizio fissate da providers multinazionali di servizi di DC ai sensi dell'art. 7.7 del CoC.	ISO/IEC 27002:2022 5.22	RID
Connettività	Linee Internet e disponibilità di banda	Previsione di misure volte ad assicurare una connettività adeguata in conformità ai livelli di servizio contrattualmente definiti con il Cliente.	ISO/IEC 27002:2022 8.6, 8.21	RI
Connettività	Firewalling	Protezione dell'accesso ai sistemi contro il rischio d'intrusione attraverso adeguate misure di firewalling.	ISO/IEC 27002:2022 5.14, 8.22, 8.21, 8.23 ISO/IEC 29100:2011 5.11	RID
Sicurezza rete	AntiDDoS	Erogazione da parte del Data Center di un servizio in grado di rispondere in modo efficace alle problematiche create dagli attacchi ("**DDoS**").	ISO/IEC 27002:2022 8.20 ISO/IEC 29100:2011 5.11	D
Sicurezza rete	IDS/IPS	Adozione di un sistema IPS (Intrusion Prevention System) in grado di bloccare automaticamente gli attacchi rilevati e IDS (Intrusion Detection System) in grado di intercettare le minacce fornendo così una protezione real-time ai servizi erogati dal Data Center.	ISO/IEC 27002:2022 8.20 ISO/IEC 29100:2011 5.11	RD
Governance	Formazione	Erogazione periodica di corsi di formazione sulla sicurezza e protezione dei dati personali ai propri dipendenti coinvolti nelle attività di trattamento.	ISO/IEC 27002:2022 6.3	na

Governance	Ubicazione geografica	Dichiarazione da parte della SWH nei confronti del Cliente dell'ubicazione geografica del DC e dei dati.	ISO/IEC 27002:2022 5.31	na
Governance	Data Breach	Adozione di procedure di individuazione, contenimento e risoluzione di situazioni di rischio (e.g. violazioni di dati personali) per la sicurezza dei dati e dei sistemi in fase post-intrusione.	ISO/IEC 27002:2022 5.5, 5.24, 5.25, 5.26, 5.27	RID
Requisiti sistemistici e di gestione	Sicurezza logica	Rivalutazione con cadenza almeno annuale delle misure e procedure di sicurezza applicate in modo da aggiornarle in relazione alle vulnerabilità rilevate, agli attacchi subiti e all'evoluzione della tecnologia.	ISO/IEC 27002:2022 8.27 MM AgID ABSC 3.1.2	RI