Indice

[1 Premessa 2](#_Toc209879632)

[2 Check list 3](#_Toc209879633)

[2.1 Misure relative all’organizzazione 3](#_Toc209879634)

[2.2 Misure relative allo sviluppo dello specifico software 3](#_Toc209879635)

[2.3 Misure relative alla funzionalità dello specifico software 4](#_Toc209879636)

[2.4 Misure relative al processo di assistenza 7](#_Toc209879637)

[2.5 Misure relative alla gestione dei sistemi e della rete 8](#_Toc209879638)

[2.6 Misure relative alla gestione del data center 8](#_Toc209879639)

[3 Misure tecniche e organizzative del Codice di condotta 10](#_Toc209879640)

[3.1 Sviluppo software 10](#_Toc209879641)

[3.2 Gestione sistemi (se dei clienti) 14](#_Toc209879642)

[3.3 Gestione sistemi (se della software house) 16](#_Toc209879643)

# Premessa

Questo documento specifica le regole da seguire per:

* sviluppo applicazioni e siti web;
* sviluppo e gestione dei server.

Le misure sono tratte dal “Codice di condotta per il trattamento dei dati personali effettuato dalle imprese di sviluppo e produzione di software gestionale”, Pubblicato sulla Gazzetta Ufficiale Serie Generale del 278 del 27 novembre 2024 e approvato con Provvedimento del garante per la protezione dei dati personali n. 618 del 17 ottobre 2024.

Nel capitolo 1 è proposta una check list con le misure del Codice di condotta, riassunte e accorpate diversamente per una più semplice consultazione.

Nel capitolo 2 sono riportate le misure del Codice di condotta, ordinate come previsto dal codice stesso e con i codici usati per un riferimento incrociato con la check list e per dimostrare che la check list è completa.

Lo schema proposto può anche essere usato per riportare ai clienti che ne volessero fare richiesta le misure di sicurezza adottate.

Il personale è tenuto a rispettare le disposizioni di questo documento.

# Check list

## Misure relative all’organizzazione

| **#** | **Requisito sintetico** | **Note di implementazione** |
| --- | --- | --- |
| C1a | Gli Amministratori di sistema (AdS) sono selezionati analizzandone le competenze e l’affidabilità. |  |
| C26 | Gli Amministratori di sistema (AdS) sono formati in merito alla gestione in sicurezza dei sistemi. |  |
| A18a | Gli sviluppatori sono formati in merito alla sicurezza dello sviluppo. |  |
| A23a | Il processo di ciclo di vita del software è documentato e include un secure development life-cycle |  |
| A11a | Sono usate di linee guida per lo sviluppo sicuro riconosciute dalla comunità degli sviluppatori (p.e. OWASP). |  |
| B19  C11  C28 | La procedura di gestione degli incidenti di sicurezza delle informazioni è documentata. |  |
| C19 | I dati sono resi al cliente su richiesta o cancellati al termine del servizio. |  |
| C20 | Nel caso di uso di fornitore per servizi sistemistici, questi è selezionato e controllato e il contratto estende ad esso gli obblighi di sicurezza presi con i clienti, applicando anche quanto previsto dall’art. 28 del GDPR. |  |
| C29 | Sono svolti audit interni periodici (annuali). |  |
| C2c | Sono svolte verifiche annuali dell’operato degli AdS. |  |
| A26b | I dati presenti negli strumenti (pc, tablet, ecc.) in uso al personale, al termine del loro utilizzo, sono cancellati in modo sicuro o sono cifrati. |  |

## Misure relative allo sviluppo dello specifico software

| **Requisito di dettaglio** | **Requisito sintetico** | **Note di implementazione** |
| --- | --- | --- |
| A1a  A1b  A1c  A2a  A2b | È mantenuto questo documento con riportati i requisiti di sicurezza per il software. |  |
| A15a | Gli ambienti di test e sviluppo sono separati da quelli di produzione. |  |
| A15b  A23b | È attivo un controllo degli accessi ai vari ambienti (identificazione, autenticazione; per l’autorizzazione, vedere il requisito successivo). |  |
| A23c | Sono stabilite e implementate le autorizzazioni per le persone che sviluppano il software e lo promuovono negli ambienti di test e produzione. |  |
| A24 | I sorgenti sono gestiti al fine di assicurare la corretta configurazione del software e il roll-back in caso di problemi di installazione in ambiente di test o produzione. |  |
| A22 | È mantenuto un inventario di librerie software. |  |
| A11b | È verificata periodicamente la disponibilità di aggiornamenti delle librerie di terze parti e, nel caso, sono installati tempestivamente. |  |
| A12b | Sono periodicamente analizzati i bollettini di sicurezza pubblici e dei fornitori. Nel caso, sono implementate tempestivamente le azioni proposte. |  |
| A12a  A13 | Se il SW è esposto su reti pubbliche, sono condotti VA-PT periodici (annuali o, se più frequente, al rilascio di ogni major release). |  |
| B11 | I test sono condotti solo con dati anonimi e non copie dei dati di produzione, tranne eccezioni documentate. |  |
| B17a | In caso di migrazione dei dati, sono usati canali cifrati. |  |
| B17b | In caso di migrazione dei dati, i db sono in ambienti ad accesso limitato. |  |
| B17c | In caso di migrazione dei dati, i dati originali sono conservati per il tempo minimo necessario (fino al buon completamento delle attività di verifica). |  |

## Misure relative alla funzionalità dello specifico software

| **Requisito di dettaglio** | **Requisito sintetico** | **Note di implementazione** |
| --- | --- | --- |
| D1 | In homepage del software è predisposto link per l’informativa fornita dal cliente.  Informative previste:   * privacy policy; * cookie policy (per siti web).   Alternativa: Informativa non necessaria. |  |
| D2 | Per i trattamenti che richiedono il consenso, l’utente ha facile accesso a funzionalità per modificarlo (p.e. per profilazione o invio pubblicità). |  |
| D3 | Per i servizi web pubblici, l’utente deve poter sempre cancellare la propria utenza e la cancellazione dell’utenza dovrebbe comportare la contestuale cancellazione di tutti i suoi dati. Se motivi legati ad adempimenti normativi o contrattuali ne impediscono l’immediata cancellazione e richiedono, quindi, la conservazione (per un periodo che deve essere comunque definito e comunicato nell’informativa), i dati devono essere “spostati” in aree diverse e separati dai dati relativi alle utenze ancora attive. |  |
| A3d  A3a | Le user-id applicative (degli utenti e degli amministratori applicativi) sono nominative e individuali. |  |
| A3d  A3b | Per gli utenti applicativi: il sistema controlla in automatico la lunghezza (minimo 8 caratteri) e la complessità (presenza di almeno un carattere speciale, lettere minuscole e maiuscole, cifre) delle password. |  |
| A3d  A4 | Possibile attivare l’uso di MFA per gli utenti applicativi. |  |
| A3d  A3c | Per gli utenti applicativi: presente un meccanismo di reset delle password con sistemi che garantiscano l’identificazione del richiedente. |  |
| A3d  A10 | Sono attivi meccanismi “standard” di protezione delle password.  Se non si usano strumenti quali MS Active Directory o similmente noti e diffusi, è verificato che le password siano conservate con meccanismi crittografici sicuri (p.e. NIST 800-63B Digital Identity Guidelines). |  |
| A3d  D4 | Tutti gli utenti possono modificare la password autonomamente quando vogliono. |  |
| A3d  A5a | Per gli utenti applicativi: è attivo un meccanismo di disattivazione delle credenziali in caso di inutilizzo per tempi prolungati (es.: sei mesi) |  |
| A3d  A5b | Per gli utenti applicativi, le credenziali sono bloccate in caso di 5 accessi falliti reiterati. Per riattivare le credenziali, devono essere contattati gli utenti amministratori.  In alternativa, le credenziali sono bloccate per un determinato periodo di tempo e viene inviato un allarme all’utente (p.e. via email) e gli utenti amministratori. |  |
| A3d  A5c | Per gli utenti applicativi, è impostato un time out della sessione attiva. |  |
| A7b | Nell’ambito dei test e dei VA-PT, è verificato che funzioni, file di dati, URL, controller e servizi non siano accessibili senza autorizzazione. |  |
| A5d | Per gli utenti applicativi è visualizzata data e ora degli ultimi accessi. |  |
| A6 | Sono attive misure di autenticazione per le API (p.e. basate su certificato digitale o token.). |  |
| A7a | Le autorizzazioni degli utenti degli amministratori applicativi sono implementate come da documentazione (A1b). |  |
| B9  B12 | Sono attive di funzionalità affinché il cliente possa selezionare le aree che il personale di assistenza può accedere o attivare gli accessi solo quando necessario. |  |
| A8 | Il cliente può accedere a un elenco dei propri utenti e delle relative autorizzazioni. |  |
| A9 | Il cliente può stabilire se cifrare i dati. |  |
| A25 | Le trasmissioni cifrate, in particolare quelle su Internet. |  |
| A14a  C3 | Attivo un log degli accessi degli utenti e amministratori applicativi e delle attività svolte. |  |
| A14b | I log sono protetti, in modo che solo gli AdS (non applicativi) possono cancellarli o modificarli.  Sono stabilite le modalità di cancellazione automatica per assicurare il non esaurimento di spazio disco. Tali modalità assicurano la disponibilità dei log per almeno 6 mesi o, quando ciò non fosse possibile, è lanciato un allarme agli AdS. |  |
| A14c | Il cliente può stabilire quali log attivare. |  |
| A5e | I log di accesso al sistema sono salvati in modo che i clienti possano esportali a sistemi terzi di conservazione. |  |
| A16 | Sono presenti funzioni che consentono ai clienti di impostare la cancellazione dei dati personali trascorso il periodo necessario di loro conservazione.  In alternativa, sono disponibili report relativi ai dati per cui sono superati i tempi di conservazione, in modo che il cliente possa decidere se cancellarli manualmente. |  |
| A17 | Presenti funzioni di estrazione dei dati in formato “comune” (p.e. .csv). |  |
| A20 | I campi di input sono progettati in modo da ridurre gli errori (p.e. date, lunghezze preimpostate, campi solo numerici o solo letterari). |  |
| A21 | Quando un utente usa funzioni di condivisione dei dati (p.e. estrazioni, invii), sono lanciati avvisi e richieste di conferma. |  |
| A19 | Sono presenti funzionalità per configurare i backup e assicurare il ripristino dei dati. |  |
| A26a | Sono controllati ed eliminati i file temporanei. |  |

## Misure relative al processo di assistenza

| **Requisito di dettaglio** | **Requisito sintetico** | **Note di implementazione** |
| --- | --- | --- |
| B18 | Per tracciare le attività di assistenza, sono usati strumenti di ticketing. |  |
| B1a  B3a  B10 | Per il personale di assistenza, è attivo un sistema di controllo della lunghezza (minimo 12 caratteri) e della complessità (presenza di almeno un carattere speciale, lettere minuscole e maiuscole, cifre) delle password usate. |  |
| B3a | Sono attivi meccanismi “standard” di protezione delle password.  Se non si usano strumenti quali MS Active Directory o similmente noti e diffusi, è verificato che le password siano conservate con meccanismi crittografici sicuri (p.e. NIST 800-63B Digital Identity Guidelines). |  |
| B4 | Le connessioni per lassistenza avvengono con VPN e MFA. |  |
| B2 | Le autorizzazioni del personale di assistenza sono gestite con un processo stabilito. Le richieste di autorizzazione e di cambiamento delle autorizzazioni sono documentate. |  |
| B8 | Nel caso in cui l’assistenza debba accedere ai sistemi e ai dati del cliente, l’autorizzazione del cliente è tracciata. |  |
| B13 | La copia o il trasferimento di dati a scopo assistenza è autorizzato preventivamente dal cliente. |  |
| B1b | È condotto un riesame periodico (almeno annuale) delle autorizzazioni per assistenza. |  |
| B5 | È assicurato il patching tempestivo della piattaforma usata per il supporto da remoto. |  |
| B6 | Le attività delle utenze privilegiate di assistenza sono tracciate e i log sono protetti. |  |
| B7 | Sono stabilite modalità di riconoscimento dell’utente che chiede assistenza (p.e. uso di strumento di ticketing a cui l’utente ha accesso con proprie credenziali personali). |  |
| B15 | In caso di copia dei db e dei dati del cliente, questi sono trasferiti su canali cifrati, salvati in ambienti ad accesso limitato e senza backup. |  |
| B14 | In caso di copia dei db e dei dati del cliente, questi sono cancellati in modo sicuro il prima possibile. |  |
| B16 | In caso di stampa di dati riservati, le stampe sono distrutte appena possibile. |  |

## Misure relative alla gestione dei sistemi e della rete

| **Requisito di dettaglio** | **Requisito sintetico** | **Note di implementazione** |
| --- | --- | --- |
| C1b | L’accesso degli AdS sistemistici avviene con VPN e MFA. |  |
| C2a | L’accesso degli AdS sistemistici avviene con credenziali personali. |  |
| C2b  C4 | Attivo un logging degli AdS sistemistici come da Provvedimento AdS del Garante privacy del 28 novembre 2008, aggiornato il 29 giugno 2009. |  |
| C5 | Le trasmissioni tra sistemi sono cifrate con strumenti standard. |  |
| C6a | Sono condotti periodici (almeno annuali) VA-PT e sono analizzati tempestivamente bollettini per identificare vulnerabilità dei sistemi. |  |
| C6b  C12 | Il patching sistemistico è tempestivo. |  |
| C7  C23 | Presente e attivo un firewall (anche L4 o L7/WAF). |  |
| C8  C25 | Attivi strumenti IDS e IPS. |  |
| C24 | È attivo un sistema anti DDoS. |  |
| C9  C10 | È usato un antimalware con controllo centralizzato. |  |
| C18 | È stabilito un piano di continuità operativa e i sistemi sono ridondati in Disaster recovery. |  |
| C22 | La connettività e il rispetto dei relativi SLA sono controllati. |  |

## Misure relative alla gestione del data center

| **Requisito di dettaglio** | **Requisito sintetico** | **Note di implementazione** |
| --- | --- | --- |
| C13  C14  C15 | Data center con controllo accessi, antincendio, anti allagamento, ecc. |  |
| C16 | Data center con CCTV. |  |
| C17 | Data center con A/C. |  |
| C21a | Il fornitore di DC è controllato con strumenti di monitoraggio. |  |
| C21b | Sono condotti audit periodici (almeno annuali) del DC. |  |
| C27 | La geolocalizzazione del DC è nota (preferibilmente nello Spazio economico europeo). |  |

# Misure tecniche e organizzative del Codice di condotta

## Sviluppo software

Misure tecniche e organizzative applicate dalle SWH per garantire i requisiti di privacy by design e by default nelle attività di sviluppo dei software gestionali.

| **Catalogazione** | **Requisito di dettaglio** | **#** |
| --- | --- | --- |
| Analisi di nuove funzioni | Valutazione e documentazione nelle analisi delle funzioni applicative del rispetto dei principi di minimizzazione:   * nel dato: ogni dato personale raccolto dal SW deve essere necessario rispetto alla finalità della raccolta * nell’uso: ogni dato personale deve essere trattato solo da coloro che ne abbiano un’effettiva necessità * nel tempo: il dato personale deve essere trattato per il tempo strettamente necessario per il perseguimento della finalità.   In particolare, già in fase di analisi devono essere identificati i dati personali trattati, la durata prevista dal trattamento, l’indicazione dei ruoli che vi potranno accedere, l’indicazione dei processi che vi potranno accedere, l’indicazione degli  output. | A1a  A1b  A1c |
| Documentazione degli strumenti e dei requisiti per l’utilizzo del SW | Documentazione degli strumenti utilizzati per trattare i dati (indicazione del DB utilizzato, strumento di scrittura del codice, sistema di conservazione dei documenti prodotti), definendo le misure di sicurezza poste a tutela dei dati (profili di accesso al DB, crittografia del DB, dialogo tra applicazione e DB e protezione delle password, ecc.).  Documentazione dei sistemi operativi e dei requisiti per l’utilizzo del SW. | A2a  A2b |
| Modalità e regole di autenticazione | Utilizzo di utenze nominative individuali al fine di garantire la tracciabilità delle operazioni eseguite.  Conformità della password policy alle best-practice europee e internazionali di riferimento che ne garantiscano sicurezza adeguata, sia in termini di complessità (es. minimo 8 caratteri presenza di caratteri speciali, maiuscole, etc.), scadenza (durata fissa o modulabile dal cliente/titolare del trattamento), ciclicità della password (es. non consentire il riuso di password precedenti), gestione reset delle password con sistemi che garantiscano l’identificazione del richiedente e simili.  Adozione di misure per prevenire e contrastare attacchi informatici di tipo credential stuffing (testing username/password pairs obtained from the breach of another site), brute force (testing multiple passwords from dictionary or other source against a single account) e password spraying (testing a single weak password against a large number of different accounts). | A3a  A3b  A3c  A3d |
| MF Authentication | MFA (quali ad es. OTP, smartcard ecc.) implementabili in base al livello di rischiosità dei trattamenti di dati personali e alle prescrizioni delle norme di riferimento. Tra i fattori di autenticazione prevedere anche la possibilità di autenticare anche il singolo device che si collega in relazione alla rischiosità del trattamento. | A4 |
| Gestione accessi | Adozione di misure che consentono di monitorare e gestire i rischi inerenti agli accessi ai sistemi applicativi, tra cui, a titolo esemplificativo:   * disattivazione delle credenziali in caso di inutilizzo per tempi prolungati (es.: sei mesi); * disattivazione temporanea o definitiva in caso di superamento di un numero impostato di tentativi di accesso falliti   reiterati;   * impostazione di time out della sessione attiva; * visualizzazione data e ora ultimi accessi;   salvataggio dei log di accesso al sistema in modo che i clienti possano esportali a sistemi terzi di conservazione che ne garantiscano l’integrità e la conservazione per i tempi definiti dai clienti stessi. | A5a  A5b  A5c  A5d  A5e |
| API | Adozione di misure di autenticazione per le API (es.: certificato digitale; token, ecc.). | A6 |
| Profili di accesso | Gestione delle utenze, sia utilizzate dal cliente per effettuare attività di amministratori del sistema (ad esempio per essere autonomi nella generazione delle utenze o nell’impostare parametri di utilizzo), sia per l’utilizzo del sistema stesso, in conformità a procedure volte a garantire il rispetto del principio di minimo privilegio e un’adeguata segregazione dei compiti gli utenti devono accedere solo a funzioni, file di dati, URL, controller, servizi e altre risorse, per le quali possiedono un'autorizzazione specifica. Le eventuali utenze generate per far accedere gli incaricati del trattamento del fornitore al fine di prestare assistenza sul prodotto utilizzato saranno identificate nominalmente e avranno profilo di  accesso amministrativo e saranno gestite dal cliente con relativa attivazione e disattivazione in caso di necessità di utilizzo. | A7a  A7b |
| Gestione delle autorizzazioni | Inventario delle utenze presenti nel sistema con i relativi profili di autorizzazione assegnati, disponibile al cliente per sua rendicontazione e analisi degli accessi. | A8 |
| Protezione dati Cliente | Adozione di tecniche di pseudonimizzazione o cifratura dei dati (tokenizzazione, etc.) adottabili dal Cliente ove appropriate allo scopo di garantire un adeguato livello di protezione in relazione alle tipologie di dati personali trattati (es.: categorie particolari ex art. 9 del GDPR e dati penali ex art. 10). | A9 |
| Protezione archivi contenenti le password | Adozione, per la conservazione delle password degli utenti, di adeguate tecniche crittografiche quali le funzioni di derivazione di chiavi crittografiche (Key Derivation Function) che offrono garanzie in caso di loro esfiltrazione dai sistemi informatici del Produttore (cfr. OWASP Password Storage Cheat Sheet, NIST 800-63B Digital Identity Guidelines). | A10 |
| Secure coding | Adozione di policy e procedure finalizzate a garantire che lo sviluppo degli applicativi avvenga nel rispetto di linee guida di secure coding conformi alle best practices (quali, ad es., OWASP, controllo delle librerie di terze parti costante e identificazione di eventuali criticità con segnalazione ai clienti e sostituzione immediata delle librerie che comportano criticità nel trattamento dei dati, etc.). | A11a  A11b |
| Minacce e Vulnerabilità | Test di penetrazione con cadenza periodica (quantomeno al rilascio di ogni major release), se il SW è destinato ad essere esposto su reti pubbliche Adozione di un piano di miglioramento che analizzi le vulnerabilità emerse dai VA e PT e dai bollettini di sicurezza pubblici e di fornitori terzi e ne preveda una adeguata gestione/risoluzione. | A12a  A12b |
| VAPT | Svolgimento periodico di analisi di vulnerabilità. | A13 |
| Log applicativi di attività utente | Funzionalità per il tracciamento del log degli accessi e delle attività svolte in relazione alle diverse tipologie di utenza (amministratore, super utente, utente, etc.) allo scopo di consentire al titolare o al responsabile del trattamento un’adeguata attività di monitoraggio. I log riguardanti le attività svolte devono essere opportunamente protetti a garanzia della loro integrità e riservatezza. Tali funzionalità devono essere attivabili da parte dell'amministratore del sistema del Cliente. | A14a  A14b  A14c |
| Misure per ambienti di test | Separazione degli ambienti di test e sviluppo rispetto ad ambienti di produzione e previsione di misure di accesso mediante  credenziali e privilegi diversi in modo di ridurre al minimo i rischi. | A15a  A15b |
| Data retention | Previsione di funzioni del SW che consentano ai clienti di impostare la cancellazione dei dati personali trascorso il periodo necessario di loro conservazione. Il SW deve prevedere estrazioni di dati che consentano ai clienti di essere consapevoli sui periodi di conservazione dei dati al fine di trattare i dati secondo il principio di minimizzazione. | A16 |
| Portabilità | Funzionalità idonee a consentire al Cliente l'estrazione dei dati personali in un formato strutturato, di uso comune e leggibile da qualsiasi dispositivo in caso di esercizio del diritto alla portabilità da parte dell'interessato, ove ne ricorrano i presupposti. | A17 |
| Formazione | Erogazione periodica alle persone autorizzate al trattamento di corsi di formazione sulla sicurezza e protezione dei dati personali. Per gli sviluppatori  sono previsti anche corsi di sviluppo sicuro. | A18a  A18b |
| Backup | Funzionalità al fine di permettere al Cliente di effettuare, anche tramite processi esterni, il salvataggio o backup dei dati trattati dall’applicativo. | A19 |
| Esattezza e accuratezza dei dati | Adozione di misure per assicurare al Cliente una verifica dell'esattezza e dell'accuratezza dei dati (ad es. controlli di correttezza formale della PIVA o CF). | A20 |
| Riservatezza dei dati | Adozione di misure per agevolare il Cliente nel rispetto del requisito della riservatezza in caso di utilizzo di funzioni di condivisione dei dati (tramite ad es. l’invio di avvisi o notifiche). | A21 |
| Inventory Librerie | Conservazione dell'inventario delle componenti software in uso comprensive delle librerie di terzi e/o open source in modo da poter rispondere più tempestivamente in caso di segnalazioni di vulnerabilità (SBOM SW bill of  materials). | A22 |
| Change management | Regolamentazione del processo di gestione delle modifiche applicative ed infrastrutturali, al fine di garantire un miglior presidio di ogni fase del ciclo di vita del SW e di tracciarne l’evoluzione, con monitoraggio dei livelli di accesso alle informazioni critiche e adeguata formazione/sensibilizzazione delle persone coinvolte nel processo di Change Management (al rispetto dei principi di *Segregation of Duties*). | A23a  A23b  A23c |
| Configuration management | Regolamentazione del processo di Configuration management al fine di garantire la corretta gestione delle versioni dei rilasci dei moduli SW. | A24 |
| Trasmissione dati personali | Utilizzo di protocolli sicuri e adeguati allo sviluppo tecnologico per proteggere i dati durante la loro trasmissione. | A25 |
| File temporanei | Funzionalità per permettere l’eliminazione dei file temporanei contenenti dati personali e creati durante i trattamenti e cancellazione sicura dei dati sugli strumenti dismessi (Secure disposal). | A26a  A26b |

## Gestione sistemi (se dei clienti)

Misure di sicurezza applicate per lo svolgimento dei servizi riguardanti i software gestionali impiegati nei contesti “on-premise”

[Le misure che seguono devono essere applicate dalla SWH qualora il software gestionale sia utilizzato dal cliente attraverso il data center del cliente stesso]

| **Catalogazione** | **Requisito di dettaglio** | **#** |
| --- | --- | --- |
| 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. | B1a  B1b |
| Assegnazione dei privilegi | L’assegnazione dei privilegi agli operatori deve avvenire in base al principio del "need-to-know" e della “segregation of duties”. | B2 |
| 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. | B3a  B3b |
| 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 comunicare al Cliente la fine dell'intervento e richiedere la disattivazione dell'accesso. | B4 |
| Patch Management | Continuo patching applicativo di sicurezza relativo alla piattaforma per l’erogazione del supporto da remoto. | B5 |
| Monitoraggio e gestione dei log di attività | Le attività svolte dagli operatori con utenze privilegiate devono essere tracciate e monitorate. | B6 |
| 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). | B7 |
| 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). | B8 |
| 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. | B9 |
| 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”). | B10 |
| 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. | B11 |
| 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. | B12 |
| 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. | B13 |
| 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. | B14 |
|  | 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. | B15 |
| 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. | B16 |
| 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. | B17a  B17b  B17c |
| Tracciabilità | Sono adottati processi e strumenti di assistenza che assicurino la tracciabilità degli interventi richiesti ed eseguiti (piattaforma di ticketing). | B18 |
| 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. | B19 |

## Gestione sistemi (se della software house)

Misure di sicurezza applicate per lo svolgimento dei servizi riguardanti i software gestionali impiegati nei contesti “on-premise”

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.

| **Catalogazione** | **Requisito di dettaglio** | **#** |
| --- | --- | --- |
| 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 ; | C1a |
| Accesso al Sistema o SW (autenticazione) | Adozione di misure dirette a garantire che:   * l’accesso amministrativo ai sistemi da parte del personale del Cliente avverrà attraverso procedure di autenticazione a più fattori (MFA). | C1b |
| 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. | C2a  C2b  C2c |
| 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. | C3 |
| 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. | C4 |
| 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. | C5 |
| 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. | C6a  C6b |
| 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. | C7 |
| 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. | C8 |
| 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). | C9 |
| 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. | C10 |
| 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. | C11 |
| 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. | C12 |
| 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.). | C13 |
| Anti allagamento | Adozione nell'ambito del Data Center di tutte le misure necessarie a prevenire allagamenti (quali presenza di sonde, impianti di allarme, ecc.). | C14 |
| 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. | C15 |
| 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. | C16 |
| Condizionamento | Adozione di adeguati impianti di condizionamento e di raffreddamento degli ambienti ed apparati. | C17 |
| 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. | C18 |
| 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. | C19 |
| 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 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). | C20 |
| 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. | C21a  C21b |
| 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. | C22 |
| Firewalling | Protezione dell'accesso ai sistemi contro il rischio d'intrusione attraverso adeguate misure di firewalling. | C23 |
| AntiDDoS | Erogazione da parte del Data Center di un servizio in grado di rispondere in modo efficace alle problematiche create dagli attacchi (“**DDoS**”). | C24 |
| 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. | C25 |
| Formazione | Erogazione periodica di corsi di formazione sulla sicurezza e protezione dei dati personali ai propri dipendenti coinvolti nelle attività di trattamento. | C26 |
| Ubicazione geografica | Dichiarazione da parte della SWH nei confronti del Cliente dell'ubicazione geografica del DC e dei dati. | C27 |
| 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. | C28 |
| 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. | C29 |