ALLEGATO 04 - Requisiti di Sicurezza

ategoria	equisito di sicurezza	Descrizione del req isito di sicurezza
Strategy, Transformation & Risk	Identificare ruoli e responsabilità in ambito Cybersecurity relativi al Servizio	Definire ruoli e responsabilità inerenti alla cybersecurity coordinati ed allineati con i ruoli interni ed i partner esterni
	Effettuare un risk assessment sul Servizio	Eseguire l'attività di risk assessment sul Servizio al fine di identificare le vulnerabilità e porvi rimedio
	Effettuare un Security Risk Assessment sulle terze parti a cui sono affidate parti dei processi relativi alla gestione del Servizio	Eseguire un Security Risk Assessment al fine di valutare e monitorare la presenza di eventuali rischi di sicurezza delle terze parti coinvolte nella gestione del servizio
	Identificare adeguate misure di sicurezza contrattuali per fornitori e terze parti	Indicare negli accordi contrattuali con i fornitori esterni le responsabilità e le misure di sicurezza in ambito sicurezza informatica appropriate alla natura e alla portata dell'accesso che avranno alle informazioni del Servizio
	Assegnare ruoli e responsabilità relativi al Servizio secondo il principio della segregation of duties	Separare i compiti, i ruoli e le aree di responsabilità in conflitto per ridurre le possibilità di modifiche non autorizzate o involontarie o di uso improprio degli asset utilizzati dal Servizio. Ogni qualvolta risulti complicato applicare il principio della segregation of duties, dovrebbero essere presi in considerazione altri controlli come il monitoraggio delle attività, audit trails e la supervisione
	Includere requisiti di sicurezza delle informazioni nella progettazione dei sistemi informativi del Servizio (security by design)	Prevedere e implementare misure di sicurezza delle informazioni all'interno dei requisiti per la definizione dei sistemi informativi del Servizio, identificando e applicando i requisiti di sicurezza delle informazioni sin dalle prime fasi di sviluppo di nuove iniziative (security by design). Progettare la sicurezza del Servizio in tutti i livelli dell'architettura (business, dati, applicazioni e tecnologia) bilanciando la necessità di sicurezza delle informazioni con la necessità di accessibilità
Security Operations	Assegnare spazio di archiviazione sufficiente per tutti i sistemi che memorizzano log	Prevedere uno storage adeguato a contenere il volume dei log generato dalle componenti del Servizio
	Utilizzare un protocollo per la sincronizzazione temporale delle componenti del Servizio per la consistenza dei timestamp dei log	Integrare il sistema di raccolta dei Log de Servizio con opportuni sistemi di sincronizzazione temporale (ad esempio NTP, PTP)
	Definire e impostare una politica di retention per i log relativi alle componenti del Servizio	Implementare un meccanismo di conservazione e relativa eliminazione dei log dopo un periodo di tempo definito
	Implementare meccanismi crittografici per proteggere riservatezza e integrità degli audit log	Prevedere dei meccanismi di hashing/cifratura a seguito della generazione del log e consentire l'accesso agli audit log solo al personale autorizzato del Servizio
	Effettuare periodicamente backup dei og	Prevedere un meccanismo di backup dei log in uno storage diverso per garantirne la disponibilità
	Prevedere un meccanismo di warning/alerting per notificare eventuali anomalie ai responsabili del Servizio in fase di logging delle componenti del Servizio stesso	Implementare Warning o Alert che notificano i responsabili del Servizio di eventuali anomalie riscontrate nel monitoraggio (ad esempio interruzione del logging da parte delle componenti, saturazione dello storage, eventuali anomalie nel formato e consistenza dei log)
	Monitorare il traffico di rete interno ed esterno generato dal Servizio	Monitorare il traffico di rete generato abilitando le funzioni di Logging nelle componenti network del Servizio per individuare prontamente eventuali anomalie nel traffico di informazioni sensibili
	Registrare nei log generati dal Servizio le seguenti informazioni rilevanti per la sicurezza del Servizio stesso: timestamp, originatore dell'evento, tipo di evento, severity (laddove possibile), descrizione (laddove possibile)	Prevedere all'interno dei log generati dalle componenti del Servizio le informazioni necessarie a garantire la riconducibilità delle azioni eseguite dagli utenti
	Monitorare le azioni eseguite dalle utenze del Servizio	Implementare un sistema integrato di monitoraggio delle azioni eseguite dalle utenze del Servizio, previa abilitazione locale dei log sulle varie componenti, affinché eventuali azioni non autorizzate possano essere tempestivamente rilevate (cambiamento delle configurazioni, azioni sui dati, azioni sulle utenze come la creazione, la modifica, l'eliminazione e l'assegnazione di privilegi)
	Monitorare gli errori generati dall'applicazione del Servizio	Monitorare gli errori generati dall'applicazione (ad esempio errori causati da richieste malformate dei client verso i Server, errori causati in fase di input dei dati, etc.) per poter mitigare eventuali anomalie ed effettuare analisi approfondite in merito a possibili incidenti di sicurezza
	Prevedere dei meccanismi di generazione dei log del Servizio	Prevedere dei meccanismi per la registrazione, il mantenimento e l'analisi dei log degli eventi, delle attività degli utenti (compresi i fornitori), delle eccezioni, dei malfunzionamenti e degli eventi relativi alla sicurezza delle informazioni per tutti i sistemi del Servizio
	Proteggere i log generati dalle componenti del Servizio	Proteggere i log generati dalle componenti del Servizio da perdita, distruzione, falsificazione e accesso non autorizzato e diffusione non autorizzata
	Applicare le patch sui sistemi utilizzati dal Servizio	Prevedere ed attuare una procedura di patch management volta all'applicazione periodica delle patch di sicurezza e degli aggiornamenti dei sistemi operativi e delle applicazioni utilizzati per il Servizio, possibilmente per mezzo di un sistema automatizzato
	Definire, applicare e testare delle procedure di backup che tengano conto del valore e della criticità delle informazioni	Stabilire, testare regolarmente ed attuare delle procedure di backup delle informazioni, del software e delle immagini dei sistemi gestiti dal Servizio che tengano conto del valore e della criticità delle informazioni, definendo la frequenza con cui effettuare i backup e la tipologia - incrementale o completa - e le misure di sicurezza da applicare a protezione delle informazioni sottoposte a backup
	Definire procedure per garantire la continuità operativa e l'affidabilità del Servizio	Definire processi e procedure per garantire la continuità operativa del Servizio e la disponibilità delle informazioni in situazioni avverse, per esempio durante crisi o disastri
	Realizzare la ridondanza delle strutture di elaborazione che costituiscono il Servizio e verificare regolarmente i controlli di continuità operativa	Garantire il soddisfacimento dei requisiti di continuità operativa e disponibilità del Servizio, realizzando strutture di elaborazione delle informazioni con sufficiente ridondanza e verificando ad intervalli di tempo regolari i controlli di continuità operativa al fine di assicurare che siano validi ed efficaci durante situazioni avverse, effettuando test di Disaster Recovery
	Prevedere un piano di ripristino del Servizio in seguito ad un incidente di sicurezza	Pianificare un piano di ripristino per garantire la continuità operativa delle componenti del Servizio in seguito a un incidente di sicurezza e comunicare alle parti interessate le varie attività che devono essere condotte. Testare tale piano, documentando tramite report di dettaglio utili a colmare eventuali gap nella tenuta di sicurezza e apportando gli interventi correttivi del caso. Tale piano di ripristino deve essere realizzato con le terze parti qualora sia demandato ad esse

ategoria	equisito di sicurezza	Descrizione el re isito i sic rezza
Identity & Access Management	Prevedere un processo di Provisioning e De-Provisioning per la gestione delle utenze del Servizio	Implementare un processo di Gestione delle Utenze per la relativa creazione, abilitazione, disabilitazione, asse nazione dei ruoli ed eliminazione, laddove applicabile
	Prevedere la presenza di un account dedicato per le attività amministrative delle utenze privilegiate	Predisporre un account dedicato nominale per l'espletamento delle attività amministrative da parte delle utenze privilegiate
	Definire un processo per la gestione delle utenze per l'accesso al Servizio	Definire e mantenere un processo per la estione dell'intero ciclo di vita delle utenze utilizzate per l'accesso al Servizio, incluse le utenze amministrative, dalla fase di creazione fino alla loro disabilitazione, che includa un inventario delle utenze e una review periodica (almeno semestrale) per la verifica della necessità o meno delle utenze del Servizio e dei relativi ruoli e privile i asse nati e che preveda delle soluzioni tecnolo iche per la estione centralizzata delle utenze
	Implementare un meccanismo di Multi-Factor Authentication per l'accesso degli utenti al Servizio	Inte rare il processo di autenticazione, sia esso locale, le ato all'Active Directory, a un'identity provider interno o esterno, con un sistema di Multi-Factor Authentication che arantisce un ulteriore livello di sicurezza per l'accesso al Servizio (come ad esempio l'utilizzo di CIE o SPID)
	Implementare controlli di anti-automation nell'autenticazione alle componenti del Servizio	Implementare meccanismi che contrastano attacchi di tipo Brute-Force nella fase di autenticazione del Servizio
	Regolamentare l'accesso ai sistemi e alle reti del servizio	Re olamentare l'accesso ai sistemi e alle reti del Servizio limitando l'accesso ai soli utenti autorizzati e ai soli servizi a cui li utenti sono autorizzati, prestando particolare attenzione alle connessioni di rete ad applicazioni sensibili o critiche
	Implementare procedure di autenticazione sicure per l'accesso ai sistemi e alle applicazioni del Servizio	Controllare l'accesso a sistemi e alle applicazioni tramite procedure di autenticazione sicure, da stabilire in base al livello di riservatezza delle informazioni elaborate dai sistemi stessi, come ad esempio soluzioni di Stron Authentication (2FA, MFA), SSO, ecc.
	Prevedere un processo per l'assegnazione e la gestione di informazioni segrete per l'autenticazione al Servizio	Prevedere un processo formale per l'asse nazione di informazioni se rete di autenticazione al Servizio, quali ad esempio le password, ma anche altre informazioni quali chiavi critto rafiche o altri dati archiviati su token hardware (ad es. smart card) che producono codici di autenticazione. Informare li utenti affinché manten ano le proprie informazioni di autenticazione se rete, non divul ando a nessuno le proprie credenziali di accesso
	Assegnare i privilegi all'interno del servizio in accordo al Principio del Privilegio Minimo	Asse nare a li utenti implicati nel Servizio un ruolo che arantisca loro i privile i minimi necessari per adempiere i loro compiti
	Prevedere il logout automatico delle utenze dopo un periodo di inattività	Asse nare un valore di timeout (da 2 minuti di inattività fino ai 30 minuti) della sessione attiva in maniera correlata alla natura del Servizio, per bilanciare sicurezza e usabilità
	Limitare il numero di sessioni simultanee in fase di autenticazione per le singole utenze del Servizio	Implementare un meccanismo per limitare il numero massimo di sessioni concorrenti per utente al Servizio
	Utilizzare algoritmi "True Random" per la generazione dei token di sessione	Utilizzare al oritmi che enerino token di sessione interamente casuali (come ad esempio ISAAC, Yarrow o EGADS) per occludere la possibilità di eventuali attacchi (es. CSRF)
	Analizzare i token di sessione ogniqualvolta l'utente richieda l'autorizzazione a svolgere qualsiasi azione all'interno del Servizio	Attuare dei meccanismi di verifica del token di sessione delle utenze ad o ni azione ese uita per attestarne l'identità e la liceità
	Prevedere un processo formale autorizzativo per assegnare i diritti di accesso privilegiato all'interno del Servizio	Prevedere un processo formale autorizzativo per l'asse nazione dei diritti di accesso privile iato al Servizio e arantire che tali diritti siano asse nati a utenti limitatamente a biso ni o eventi specifici, secondo il principio del privile io minimo. Verificare re olarmente le competenze de li utenti con diritti di accesso privile iati per verificare che siano in linea con le loro mansioni
Threat & Vulnerability Management	Condurre un Vulnerability Assessment e un Penetration Test prima del rilascio in produzione del Servizio	Ese uire un Vulnerability Assessment e Penetration Test prima del rilascio in produzione del Servizio, con relativa formalizzazione di report con i risultati delle analisi e di piani di rientro dalle vulnerabilità riscontrate
	Gestire le vulnerabilità di sicurezza sui sistemi del Servizio	Stabilire e mantenere una procedura per la estione delle vulnerabilità di sicurezza sui sistemi del Servizio, che preveda l'esecuzione di scansioni automatizzate delle vulnerabilità dei sistemi e delle risorse estite dal Servizio, su base periodica, determinata in base alla criticità dei sistemi da scansionare. Le scansioni andrebbero ese uite anche dopo aver applicato i piani di fix emersi, in modo da verificare sul campo il rientro delle vulnerabilità
	Correggere le vulnerabilità rilevate nei sistemi del Servizio	Prevedere delle procedure per la correzione delle vulnerabilità rilevate nei sistemi del Servizio, con l'obiettivo di miti are il livello di esposizione al rischio degli stessi
	Garantire che le componenti del Servizio utilizzino l'ultima stable release del software	Adottare tool per la verifica e l'installazione costanti delle ultime stable release/aggiornamenti disponibili per il software
	Implementare un servizio di threat intelligence	Implementare un servizio automatizzato di threat intelli ence per individuare tempestivamente l'attivarsi di minacce o pericoli esistenti/noti o emergenti per le risorse/asset del Servizio
	Ricevere informazioni su minacce e vulnerabilità da fonti esterne relative alle componenti utilizzate dal Servizio	Implementare un meccanismo di ricezione automatica delle nuove minacce world-wide per poter definire prontamente eventuali contromisure nella scoperta di una nuova vulnerabilità che potrebbe impattare la sicurezza di una componente del Servizio

Categoria	Requisito di sicurezza	Descrizione del requisito di sicurezza
Data Security	Implementare un meccanismo di verifica dell'integrità dei dati at-rest del Servizio	Implementare un meccanismo che, rilevando e valutando possibili violazioni dell'integrità dei dati at-rest del Servizio, automaticamente attivi una reazione proporzionale all'entità di quest'ultima
	Implementare un meccanismo di verifica dell'integrità dei dati in-transit del Servizio	Implementare un meccanismo che, rilevando e valutando possibili violazioni dell'integrità dei dati in-transit del Servizio, automaticamente attivi una reazione proporzionale all'entità di quest'ultima
	Garantire che l'output dell'applicazione del Servizio mostri le informazioni pertinenti e conformi alle richieste avanzate dagli utenti in modo da garantire il principio di Riservatezza delle informazioni stesse	Assicurare che l'applicazione fornisca in output solamente le informazioni pertinenti e conformi alle richieste avanzate dagli utenti, al fine di evitare qualsiasi raccolta d'informazioni (information gathering) o rivelazione di dati (disclosure) non autorizzate
	Ottenere certificati utilizzati dal Servizio da una CA autorizzata	Identificare e adottare una Certification Authority autorizzata per l'emissione dei certificati utilizzati dal Servizio
	Sanificare i supporti rimovibili prima del loro utilizzo inerente al Servizio	Condurre la sanificazione di tutti i dispositivi rimovibili nuovi, per eliminare possibili minacce insite nel prodotto, eseguendo tale operazione precedentemente all'implementazione della cifratura
	Assicurare la privacy e la protezione dei dati personali	Definire una politica in materia di protezione dei dati personali e adeguati ruoli e responsabilità inerenti al trattamento e la protezione dei dati personali per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner), prevedendo in quest'ultimo caso la nomina a Responsabile del trattamento.
	Stabilire processi per la nomina delle figure coinvolte nel trattamento dei dati personali, predispondendo percorsi di formazione	Definire processi per la nomina delle figure coinvolte nel trattamento dei dati personali, siano esse figure interne o esterne, riesaminando/aggiornando periodicamente tali nomine. Predisporre, inoltre, per coloro che hanno accesso ai dati personali percorsi di formazione differenziati in relazione alle loro mansioni
	Regolamentare il trasferimento sicuro delle informazioni con le "terze parti"	Accordarsi con le "terze parti" per quanto riguarda il trasferimento sicuro delle informazioni, anche tramite la stipulazione di contratti per formalizzare, ad esempio, gli accordi di riservatezza o di non divulgazione dei dati
	Nominare un Responsabile per la protezione dei dati personali (Data Protection Officer - DPO) (rif artt. 37, 38, 39 del GDPR)	Nominare un DPO che sarà coinvolto in tutte ciò che riguarda il trattamento di dati personali all'interno dell'organizzazione, incluse le seguenti attività: controllo del rispetto della normativa nazionale ed europea in materia di protezione dei dati personali, consulenza al personale in materia di protezione dei dati, relazione con le Autorità di controllo e gli interessati
	Definire l'informativa recante disposizioni sulle modalità di trattamento dei dati personali degli interessati (rif artt. 6, 12, 13, 14 del GDPR)	Definire l'informativa per il trattamento dei dati personali degli interessati in modo che le informazioni relative al trattamento siano fornite all'interessato in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro
	Prevedere delle procedure per consentire agli interessati di esercitare i propri diritti (rif artt. 15-22 del GDPR)	Definire e implementare delle procedure per consentire agli interessati di esercitare i propri diritti, in particolare: a) il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali; b) il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano; c) il diritto di ottenere la cancellazione dei dati personali che lo riguardano; d) il diritto di ottenere ottenere la limitazione del trattamento; e) il diritto di ricevere i dati personali che lo riguardano, forniti a un titolare del trattamento, e di trasmetterli a un altro titolare del trattamento; f) il diritto di opporsi al trattamento dei dati personali che lo riguardano
	Se Titolare del trattamento, garantire e dimostrare la conformità del trattamento rispetto al regolamento GDPR (rif art 24 del GDPR)	Il Titolare del trattamento deve garantire e dimostrare la conformità del trattamento rispetto al regolamento GDPR, dimostrando il soddisfacimento di tale requisito tramite misure tecniche e organizzative adeguate
	Mettere in atto misure di protezione dei dati personali (rif art 32 del GDPR)	Attuare misure di protezione dei dati personali (ad es: cifratura) per garantire un livello di sicurezza adeguato ai rischi, tra cui quelli di distruzione, perdita, modifica e divulgazione dei dati personali
	Prevedere e garantire il rispetto del principio di "privacy-by-design-default" (rif art 25 del GDPR)	Integrare i requisiti per la protezione dei dati personali nell'intero ciclo di vita di una tecnologia, fin dalla primissima fase di progettazione
	Prevedere la notifica di una eventuale violazione di sicurezza dei dati personali all'Autorità di Controllo competente (rif artt 33-34 del GDPR)	Prevedere un meccanismo di notifica di un'eventuale violazione di sicurezza dei dati personali all'Autorità di Controllo competente, da effettuare, se possibile, entro 72 ore dall'avvenuta conoscenza della violazione. Per violazione di sicurezza si intende un qualsiasi evento che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trattati
	Definire un registro dei trattamenti del titolare (rif art 30 del GDPR)	Definire un documento per il censimento dei trattamenti effettuati in qualità di Titolare del trattamento, ed un registro dei trattamenti del responsabile, ossia un documento per il censimento dei trattamenti effettuati per conto di titolari esterni all'organizzazione
	Attuare la DPIA (Data Protection Impact Assessment) (rif art 35 del GDPR)	Attuare l'attività di DPIA (Data Protection Impact Assessment) qualora un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche
	Documentare tutti i processi di trasferimento dei dati personali in ambito internazionale (rif artt 44-49 del GDPR)	Definire ed implementare i suddetti processi, con relativa attuazione delle misure di sicurezza a protezione del trasferimento stesso
	Garantire che l'eventuale presenza di dati di produzione negli ambienti di sviluppo e test sia approvata, documentata, monitorata	Scegliere i dati di test con attenzione, proteggendoli e tenendoli sotto controllo, evitando l'uso di dati contenenti informazioni di identificazione personale o qualsiasi altra informazione riservata per scopi di test
	Cifrare i dati at-rest del Servizio	Garantire, tramite opportuni sistemi di cifratura adeguatamente complessi, la riservatezza dei dati 'at-rest'
	Cifrare i dati in-transit del Servizio	Garantire, tramite opportuni sistemi di cifratura adeguatamente complessi, la riservatezza dei dati 'in-transit' e 'in-use'
	Proteggere le chiavi crittografiche utilizzate dal Servizio	Proteggere adeguatamente le chiavi crittografiche utilizzate nel Servizio. In particolare, è necessario garantire la riservatezza, l'integrità e disponibilità per le chiavi private, e l'integrità e disponibilità per quelle pubbliche
	Cifrare i supporti rimovibili utilizzati dal Servizio	Implementare la cifratura di tutti i dispositivi rimovibili aziendali, affinché i dati in essi conservati siano protetti
	Definire ed attuare una policy sull'uso e sull'applicazione della crittografia per la protezione delle informazioni	Analizzare i dati in modo tale da identificare quelli con particolari requisiti di riservatezza e di conseguenza quelli ai quali va applicata la protezione crittografica. Stabilire una politica sull'uso, sulla protezione e sulla durata delle chiavi crittografiche attraverso il loro intero ciclo vita
	Prevedere un meccanismo formale per l'eliminazione sicura dei dati gestiti e non più necessari al Servizio	Assicurarsi che ogni dato e/o software sia rimosso o sovrascritto in modo sicuro prima della dismissione o del riutilizzo dell'asset, mediante, ad esempio wiping dei dischi utilizzati (DoD short), PRNG Stream o de-magnetizzazione
	Definire un periodo di retention dei dati gestiti dal Servizio	Definire e rispettare un periodo di retention dei dati gestiti dal Servizio, in accordo con le normative e gli obblighi cogenti
	Proteggere i supporti rimovibili utilizzati dal Servizio	Prevedere dei meccanismi di protezione dei supporti rimovibili utilizzati dal Servizio, con relativa restrizione all'utilizzo

Categoria	Requisito di sicurezza	Descrizione del requisito di sicurezza
Software & Application Security	Proteggere l'application web del Servizio mediante Web Application Firewall	Predisporre l'implementazione di WAF (Web Application Firewall) per filtrare il traffico dati verso l'applicazione web del Servizio, a prevenzione dei principali attacchi
	Eliminare o oscurare informazioni sensibili presenti nel codice sorgente prima del rilascio in produzione del Servizio	Definire procedure sicure di scrittura del codice del Servizio - appropriate al linguaggio di programmazione e all'ambiente di sviluppo in uso - ponendo particolare attenzione all'esclusione di qualunque informazione relativa ai dati di accesso dal codice sorgente del Servizio stesso (ad esempio username, password, nome DB, nome server, etc.)
	Implementare meccanismi di difesa contro l'HTTP Pollution	Implementare meccanismi atti ad impedire l'inserimento di parametri multipli aventi lo stesso nome nelle richieste HTTP dell'applicazione del Servizio
	Abilitare gli attributi "HttpOnly", "Secure" e "SameSite" nella generazione dei cookies	Abilitare gli attributi "HttpOnly", "Secure" e "SameSite" nella generazione dei cookies. Tali cookies devono scadere dopo un timeout limitato oltre il quale non devono più esser considerati validi
	Implementare meccanismi di controllo dei campi di input dell'applicazione per verificare che le informazioni inserite dagli utenti siano congruenti con quanto atteso dal Servizio	Implementare meccanismi di controllo e validazione dell'input (espressioni regolari, whitelisting - da preferire al blacklisting -, validazione stringa, ecc.), anche in fase di autenticazione (contro SQL Injection), per garantire che solo valori congruenti e completi siano inseriti, e al tempo stesso evitare l'upload di file malevoli (Local File Injection, Remote File Injection)
	Separare logicamente e fisicamente l'ambiente di sviluppo e test da quello di produzione del Servizio	Prevedere che gli ambienti di test e sviluppo del Servizio siano logicamente e fisicamente separati "by-design" dall'ambiente di produzione, applicando a ciascuno di questi le configurazioni più adatte
	Proteggere il codice sorgente e le librerie utilizzate nello sviluppo dell'applicazione del Servizio	Prevedere ed implementare controlli del codice sorgente, atti a rilevare eventuali anomalie (code injection), nonché porzioni di codice potenzialmente malevolo (backdoor). Va inoltre garantito che i sorgenti e le librerie dell'applicazione del Servizio all'interno dei sistemi di esercizio siano presenti come oggetti compilati e mai in chiaro
	Gestire gli errori e le eccezioni nello sviluppo dell'applicazione del Servizio	Prevedere la definizione ed implementazione di un sistema di gestione degli errori e delle eccezioni dell'applicazione del Servizio per evitare di mostrare informazioni sensibili a un attaccante (Information Leak) o consumare risorse in maniera eccessiva (Excessive resource consumption, DOS)
	Effettuare SAST e DAST sul codice del Servizio prima del rilascio in produzione	Prevedere l'esecuzione sistematica e strutturata di SAST (Static Application Security Testing) e DAST (Dynamic Application Security Testing) sul codice del Servizio, anche nel caso in cui il relativo sviluppo sia demandato a terze parti, prima di ciascun rilascio in produzione
	Utilizzare Secure Random Number Generator nella creazione di valori casuali all'interno delle funzioni nello sviluppo dell'applicazione del Servizio	Adottare nell'applicazione del Servizio Secure Random Number Generator ogniqualvolta le funzionalità richiedano l'utilizzo di valori random nello sviluppo del codice (ad esempio utilizzare funzioni robuste per la generazione di one-time password o altri codici di sicurezza)
	Impedire l'Overflow nello sviluppo del codice del Servizio	Evitare nello sviluppo applicativo del codice del Servizio la possibilità di causare Overflow, ad esempio configurando i cicli sugli array in modo da non superare il numero di elementi previsto o evitando cicli ricorsivi nel codice
	Utilizzare algoritmi crittografici nella generazione delle OTPs utilizzate dall'applicazione del Servizio	Utilizzare algoritmi crittografici nella generazione delle OTPs utilizzate dall'applicazione del Servizio

Categoria	Requisito di sicurezza	Descrizione del requisito di sicurezza
Infrastructure Security	Implementare meccanismi di mutua autenticazione nei nodi del Servizio laddove possibile	Autenticare entrambi i nodi in ogni comunicazione in cui il Servizio è coinvolto, sia back-end, front-end e cross tra le due, per inibire la possibilità di attacchi informatici. Qualora i due nodi comunichino mediante un canale dedicato, la mutua autenticazione è automaticamente adempiuta
	Proibire, laddove possibile, l'esecuzione di binari ed eseguibili nelle componenti del Servizio	Disabilitare l'esecuzione di script, binari o eseguibili nelle componenti del Servizio dove essa non è prevista, per prevenire la possibilità di esecuzione impropria del codice
	Disabilitare, laddove possibile, tutte le funzionalità/componenti non necessari ai fini dell'erogazione del Servizio	Disabilitare tutte le componenti non necessarie al Servizio con l'obiettivo di ridurre l'Attack Surface. Prevedere dunque, laddove possibile, le seguenti azioni: -disabilitazione di porte e servizi non necessari -eliminazione plug-in/add-on non necessari -eliminazione, prima del rilascio in produzione, di utenze standard, utenze con password di default o utenze non utilizzate dal Servizio -disabilitazione nell'applicazione web del Servizio del metodo "HTTP Trace"/TRACK -disabilitazione delle funzionalità potenzialmente pericolose di XML all'interno dell'applicazione del Servizio -disabilitazione della Keyboard Cache dell'applicazione mobile del Servizio -disabilitazione del Directory Listing nelle componenti Server del Servizio
	Stabilire una procedura di hardening per la sicurezza dei sistemi IT, compresi i sistemi per l'elaborazione delle informazioni deployati in cloud	Definire una procedura di hardening dei sistemi IT che comprenda misure di sicurezza come ad esempio: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, applicazione di patch, chiusura di porte di rete aperte e non utilizzate, ecc.
	Prevedere un software anti-virus e anti-malware a protezione delle componenti del Servizio	Adottare un software anti-virus e anti-malware per proteggere le componenti utilizzate dal Servizio
	Autorizzare le connessioni interne tra le componenti del Servizio	Prevedere un meccanismo per l'autorizzazione non solo delle componenti esterne che si connettono al Servizio, ma anche di tutte le richieste provenienti da rete interna
	Limitare il numero di connessioni simultanee al Servizio provenienti dalla rete esterna	Definire un limite di connessioni esterne concorrenti che il Servizio può gestire, al fine di limitarne la consumazione di risorse e relativi attacchi informatici (ad esempio DDOS)
	Segregare la rete del Servizio	Prevedere la segregazione logica o fisica dei sistemi del Servizio così da aumentare la protezione delle singole componenti e da controllare più efficacemente i flussi di informazioni
	Verificare e revisionare periodicamente le misure di sicurezza contrattualizzate con il cloud provider	Verificare e revisionare periodicamente tutte le misure di sicurezza contrattualizzate con il cloud provider in merito alla loro validità
	Stabilire un processo di dismissione sicura degli asset usati in ambiente cloud	Implementare un processo di dismissione sicura degli asset usati dal Servizio in ambiente cloud, includendo server, macchine virtuali, storage, ed in generale qualsiasi dato e/o informazione elaborati
	Prevedere ed attuare delle procedure per il monitoraggio dei servizi erogati dal cloud provider	Monitorare i servizi erogati dal cloud provider, ad esempio attraverso la definizione di KPI e SLA
	Implementare strategie e funzionalità per una distribuzione delle applicazioni sicura	Definire e implementare strategie per una distribuzione delle applicazioni in modalità sicura, standardizzata, conforme e automatizzata (deployment e integrazione del codice)
	Seguire un processo definito per il controllo delle modifiche, approvazione e test di qualità	Definire un processo per il controllo delle modifiche, approvazione e test di qualità con linee di guida, test e standard di rilascio stabiliti
	Implementare ruoli e responsabilità in materia di crittografia, cifratura e gestione delle chiavi	Definire e implementare ruoli e responsabilità in materia di crittografia, cifratura e gestione delle chiavi, specificando le responsabilità e i requisiti di accesso nel caso di soluzioni BYOK (Bring Your Own Key) e HYOK (Hold Your Own Key)
	Utilizzare librerie crittografiche accettate dal settore per la creazione di chiavi crittografiche	Generare chiavi crittografiche utilizzando librerie crittografiche accettate dal settore, specificando la forza dell'algoritmo e il generatore di numeri casuali utilizzato.
	Ruotare le chiavi crittografiche in base al criptoperiodo calcolato	Stabilire un adeguato cryptoperiod per ogni chiave crittografica, tenendo conto del rischio di divulgazione delle informazioni e dei requisiti legali e normativi, e ruotare le chiavi in base al cryptoperiod definito
	Implementare e valutare i processi, le procedure e le misure tecniche per revocare e rimuovere le chiavi crittografiche	Nel caso in cui questo debba avvenire prima della fine del periodo di crittografia stabilito, quando una chiave è compromessa o un'entità non fa più parte dell'organizzazione, includendo disposizioni per i requisiti legali e normativi
	Implementare sistemi di sorveglianza dei data center	Implementare, mantenere e garantire il funzionamento dei sistemi di sorveglianza del data center sul perimetro esterno e in tutti i punti di ingresso e di uscita per rilevare i tentativi di ingresso e di uscita non autorizzati
	Gestire le richieste di divulgazione di dati personali da parte delle autorità	Il CSP deve disporre e descrivere ai CSC la procedura per gestire e rispondere alle richieste di divulgazione dei dati personali da parte delle autorità preposte all'applicazione della legge, in conformità alle leggi e ai regolamenti applicabili. Il CSP deve prestare particolare attenzione alla procedura di notifica ai CSC interessati, a meno che non sia altrimenti vietato, come ad esempio il divieto previsto dal diritto penale di preservare la riservatezza di un'indagine delle forze dell'ordine
	Definire e implementare processi, procedure e misure tecniche per specificare e documentare le ubicazioni fisiche dei dati	Definire e implementare processi, procedure e misure tecniche per specificare e documentare le ubicazioni fisiche dei dati, comprese le ubicazioni in cui i dati vengono elaborati o sottoposti a backup
	Garantire l'accesso privilegiato limitato nel tempo	Definire e implementare un processo di accesso per garantire che i ruoli e i diritti di accesso privilegiato siano concessi per un periodo di tempo limitato
	Limitare l'accesso tenant e intra-tenant	Progettare, sviluppare, distribuire e configurare applicazioni e infrastrutture in modo che l'accesso degli utenti CSP e CSC (tenant) e l'accesso intra-tenant siano adeguatamente segmentati e segregati, monitorati e limitati rispetto agli altri tenant
	Utilizzare canali di comunicazione sicuri per la migrazione in ambienti cloud	Utilizzare canali di comunicazione sicuri e criptati tramite protocolli aggiornati e approvati durante la migrazione di server, servizi, applicazioni o dati in ambienti cloud
	Implementare la defense-in-depth per prevenire gli attacchi basati sulla rete	Definire, implementare e valutare processi, procedure e tecniche di defense-in-depth per la protezione, il rilevamento e la risposta tempestiva agli attacchi basati sulla rete
	Definire processi per l'esecuzione periodica di test di penetrazione	Definire, implementare e valutare processi, procedure e misure tecniche per l'esecuzione periodica di test di penetrazione da parte di terzi indipendenti