TRENTINO DIGITALE S.P.A.

Sicurezza nella progettazione e sviluppo di soluzioni informatiche

PRINCIPALI MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE

Data	Versione	Modifiche apportate
	01.0 Obsoleta	Prima emissione
	01.1 Obsoleta	Integrazione dei riferimenti alle procedure ITIL del SGQ e modifica definizione *Dato Personale* sulla base dall'art. 40, comma 2, lettera a), del decreto legge 6 dicembre 2011, n. 201, convertito, con modificazioni, dalla legge 22 dicembre 2011, n. 214..
	01.2 Obsoleta	Aggiornamento riferimenti SGQ a seguito soppressione SGQ-PR-90, SGQ-PR-05 e SGQ-PR-07 sostituite dalle SGQ-PR-90.1, SGQ-PR-91.1, SGQ-PR-22.2 e SGQ-PR-22.2
	01.3 Obsoleta**ERRORE. IL SEGNALIBRO NON È DEFINITO.**	Aggiornamento riferimenti normativi a seguito del D.Lgs. 101/18
19/09/2019	02.00 Obsoleta	Aggiornamento template e contenuto del documento
16/10/2020	02.1 In vigore	Adeguamento a seguito dell'adozione dei controlli previsti dalle norme ISO/IEC 27017:2015 e ISO/IEC 27018:2014

INDICE

1 Introduzione

1.1 Premessa

Obiettivo del presente documento è fornire le linee guida che devono essere adottate per integrare gli aspetti di sicurezza delle informazioni (vedi documento SIC-POL-08 "*Sicurezza nella progettazione e sviluppo di soluzioni informatiche*") in tutte le fasi legate alla progettazione e allo sviluppo di soluzioni informatiche, descritte all'interno dei documenti SGQ-PR-22.2 "Progettazione e realizzazione di componente di servizio" e SGQ-PR-22.3 "Progettazione e sviluppo di servizi ICT".

1.2 Perimetro organizzativo

La presente linea guida si applica a tutto il personale dipendente di Trentino Digitale e a tutti i soggetti che collaborano con Trentino Digitale impegnati nello sviluppo e nella produzione di soluzioni informatiche.

1.3 Termini e definizioni

Asset – Qualsiasi risorsa che abbia un valore per l'organizzazione (es. informazioni e dati, software, beni fisici..)

Cloud – Un insieme di servizi ICT accessibili on-demand e in modalità self-service tramite tecnologie Internet, basati su risorse condivise, caratterizzati da rapida scalabilità e dalla misurabilità puntuale dei livelli di performance, in modo da poter essere pagati in base al consumo.

Cloud Privato– Piattaforma basata su Cloud gestita internamente per erogare servizi e non aperta alla disponibilità di soggetti terzi.

Cloud Pubblico – Piattaforma basata su Cloud che eroga servizi a più soggetti non connessi tra di loro.

Cloud Ibrido – Soluzione tecnologica che prevede l'impiego combinato di Cloud Pubblico e Cloud Privato.

Dato Personale - qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dato particolare - dato personale che rivela l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Infrastruttura tecnologica – complesso dei sistemi di elaborazione (hardware, software di base e middleware) e dei sistemi di telecomunicazione mediante i quali sono erogati i servizi informatici.

Recovery Point Objective (RPO) - perdita dati sostenibile, in termini di distanza temporale tra il verificarsi dell'emergenza e l'ultimo salvataggio utile e ripristinabile dei dati.

Recovery Time Objective (RTO) - Tempo disponibile per il recupero dell'operatività di un sistema o di un processo organizzativo.

Servizio informatico – Il servizio è un mezzo attraverso il quale poter fornire valore ai clienti facilitando i risultati che i clienti desiderano conseguire senza sostenere gli specifici costi e rischi.(*Foundations of IT Service Management based on ITIL v3, 2007*)

Software applicativo – insieme dei programmi che vengono realizzati e installati per svolgere attività specifiche.

Single Point of Failure (*SPoF*) – Componente di un sistema informativo che, in caso di malfunzionamento/guasto, provoca il blocco dell'intero sistema.

Trattamento di Dati - qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Vulnerabilità – Debolezza intrinseca di un componente del sistema informativo della società che può essere sfruttata da una minaccia per arrecare un danno ai beni dell'organizzazione

1.4 Riferimenti

Norme di legge	*Regolamento (UE) 2016/679 "Regolamento generale sulla protezione dei dati"* *D.lgs. 196/2003 "Codice in materia di protezione dei dati personali" e ss. mm. ii.* Provvedimento del Garante privacy del 27/11/2008 recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008"*
Standard di Riferimento	UNI CEI ISO/IEC 27001:2014 – *"Tecnologia per l'Informazione – Tecniche per la Sicurezza – SGSI - Requisiti"* ISO/IEC 27017:2015 – *"Information technology - Security*

	techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services" ISO/IEC 27018:2015 – *"Information technology – Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors"* *Foundations of IT Service Management based on ITIL v3, 2007*
A documenti del Sistema Sicurezza	SIC-LG-06 *"Sviluppo sicuro: principali minacce e relative contromisure"* SIC-POL-04 *"Aspetti contrattuali connessi con la sicurezza delle informazioni"* SIC-POL-08 "*Sicurezza nella progettazione e sviluppo di soluzioni informatiche*" SIC-STD-06 *"Classificazione e gestione degli asset"*
A documenti del Sistema di Gestione della Qualità	SGQ-PR-35.1 "*Capacity Management*" SGQ-PR-50.3 "*Access Management*" SGQ-PR-90.1 "*Service Catalogue management*" SGQ-PR-91.1 "*Service Asset and Configuration management*" SGQ-PR-22.2 "*Progettazione e realizzazione di componente di servizio*" SGQ-PR-22.3 "*Progettazione e sviluppo di servizi ICT*"

2 Linee Guida

Nei seguenti paragrafi sono presentate le linee guida di sicurezza delle informazioni che devono essere considerate nella progettazione di servizi ICT, costituiti generalmente da soluzioni applicative e infrastrutture tecnologiche. Si precisa che le linee guida devono essere applicate in modo contestuale alla tipologia del servizio considerato, sia esso gestito in house o su Cloud Pubblico, perseguendo l'obiettivo di adottare misure di sicurezza, tanto tecniche quanto organizzative, adeguate alla criticità dei dati trattati.

2.1 Definizione requisiti e proposta

L'attività ha l'obiettivo di individuare e definire i requisiti posti dal cliente (interno o esterno), quelli non precisati ma necessari, quelli derivanti da norme cogenti e/o stabilite dall'azienda: le strutture responsabili dell'interfacciamento con il cliente devono recepire le esigenze dello stesso e tradurle in requisiti e successivamente definire la proposta di soluzione che li soddisfi tutti.

2.1.1 Requisiti per la progettazione di una componente applicativa

Di seguito sono riportate le linee guida di sicurezza e/o misure/specifiche legate alla progettazione di una componente applicativa.

2.1.1.1 Criteri per l'autenticazione

Per garantire una corretta autenticazione degli utenti e/o delle entità (es. processi inter-applicativi e batch) che devono accedere all'applicazione, occorre rispettare i seguenti criteri:

- prevedere i necessari meccanismi di autenticazione al fine di garantire che solo gli utenti/entità autorizzate possano accedere ai dati trattati dall'applicazione, garantendo adeguati livelli di riservatezza;
- privilegiare l'utilizzo di meccanismi di autenticazione esterni alle applicazioni, evitando che le funzionalità di autenticazione siano parte del codice applicativo:
    - impiegando procedure e componenti infrastrutturali, centralizzati e/o condivisi da più applicazioni (per es. LDAP, Active Directory, ecc.);
    - evitando di archiviare le informazioni di autenticazione in basi dati proprie o in file permanenti;
- progettare i sistemi di autenticazione alle applicazioni in modo che le modalità di autenticazione siano conformi alla normativa vigente e alle policy interne, in particolare:
    - consentire l'accesso a funzionalità non considerate di pubblico accesso solo previo superamento di una procedura di autenticazione, basata almeno su un set di credenziali (user-ID e password);
    - prevedere che ad ogni incaricato possano essere assegnate o associate individualmente una o più credenziali per l'autenticazione;

- prevedere meccanismi di gestione e controllo delle password che inibiscano l'utilizzo di password non conformi alle regole di lunghezza (non inferiore ad 8 caratteri), scadenza (non superiore ai 6 mesi in caso di trattamento di dati personali e 3 mesi in caso di dati personali particolari) e di composizione/qualità (utilizzo di caratteri maiuscoli/minuscoli/numeri etc.);
- consentire la modifica autonoma delle password da parte dell'utente, inibendo il riuso almeno della password precedente ed ulteriori sostituzioni della password prima di un limite temporale minimo prefissato;
- prevedere la disattivazione, nel caso di trattamento di dati personali, delle credenziali non utilizzate da un periodo prefissato pari a 180 giorni;
- mascherare i caratteri della password durante la digitazione da parte dell'utente;
- prevedere la trasmissione di User-ID e password o, in generale, di credenziali di accesso, in modo sicuro utilizzando protocolli cifrati;
- proteggere crittograficamente le password, preferibilmente utilizzando una funzione non invertibile (hashing).

2.1.1.2 Criteri per l'autorizzazione

Per garantire una corretta profilazione degli utenti e/o delle entità (es. processi inter-applicativi e batch) che devono accedere all'applicazione devono essere considerati i seguenti criteri:

- definire dei meccanismi di autorizzazione tali da garantire che gli utenti e/o le entità autorizzate accedano alle sole informazioni e funzionalità essenziali (lettura, scrittura, modifica, cancellazione) per la loro operatività, applicando il criterio del "minimo privilegio" (ogni utente deve essere in grado di effettuare le sole operazioni necessarie per l'espletamento della propria attività);
- prevedere dei profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, privilegiando strutture per la gestione dei profili di accesso basate su ruoli (rif. SGQ-PR-50.3 "*Access Mangement*");
- progettare le applicazioni favorendo, laddove risulti possibile, l'utilizzo di meccanismi di autorizzazione esterni alle stesse e comunque in generale:
  - evitando che le funzionalità di autorizzazione siano parte del codice applicativo;
  - non consentendo la modifica delle informazioni di autorizzazione da parte dell'applicazione stessa.

2.1.1.3 Criteri per la gestione delle attività degli utenti

In termini di specifiche utente occorre individuare e definire i seguenti elementi:

- tutti gli accorgimenti necessari per una corretta gestione delle sessioni utente (es. prevedere time-out di sessione dopo un prefissato periodo di inattività dell'utente, definendo dei

meccanismi di blocco o sospensione/disconnessione automatica; prevedere la generazione cookie e ID di sessione sicuri e non prevedibili);

- il numero massimo di tentativi di accesso falliti accettabili e le conseguenti operazioni (ad esempio blocco del corrispondente account per 15 minuti);
- il tempo massimo di inutilizzo prolungato di un account accettabile e le conseguenti operazioni (ad esempio disconnessione del corrispondente account);
- gli intervalli orari di connessione all'applicazione (eventualmente anche 24 ore su 24 per 7 giorni se l'applicazione deve essere sempre disponibile);
- un limite per il numero massimo di accessi contemporanei all'applicazione da parte della stessa utenza.

2.1.1.4 Criteri per la validazione dei dati in input/output

In termini di validazione dei dati in input/output occorre prendere in considerazione ed eventualmente definire i seguenti elementi:

- opportuni controlli da eseguire per tutti i dati forniti dagli utenti al fine di assicurarsi che siano appropriati e consistenti rispetto a quanto atteso (ad es. in relazione al tipo e/o al formato e/o alla dimensione dei dati) e che non sia accettato altro tipo di dati;
- opportuni controlli dell'output prodotto dall'applicazione per assicurarsi che le elaborazioni effettuate siano corrette e complete rispetto a quanto atteso;
- meccanismi di tracciatura per controllare la corretta esecuzione delle verifiche e dei controlli sopra descritti, così da monitorare le eventuali anomalie avvenute;
- opportune segnalazioni circa l'occorrenza di qualsiasi condizione anomala quale sia un errore o un'eccezione o altri meccanismi equivalenti;
- prevedere, là dove necessari e tecnicamente possibili, controlli automatici da attuare durante le elaborazioni dati (per es. quadrature, ecc.) od in sostituzione eventuali controlli manuali ad integrazione.

(per i dettagli in merito alle principali minacce e relative contromisure fare riferimento al documento SIC-LG-06 "*Sviluppo sicuro: principali minacce e relative contromisure*")

2.1.1.5 Criteri per l'utilizzo di meccanismi crittografici

L'utilizzo di meccanismi crittografici, qualora non fosse esplicitamente richiesto per adempiere a vincoli legislativi, deve essere sempre valutato in funzione dei costi associati a tali tecnologie. In alcuni casi, essendo il beneficio introdotto dall'utilizzo della crittografia inferiore ai suoi costi, è possibile adottare dei criteri alternativi (es. la separazione dei dati particolari dagli altri dati personali trattati per diverse finalità).

Nello specifico, la valutazione circa l'opportunità, o meno, di utilizzare la cifratura per la protezione dei dati trattati dalle applicazioni e/o delle componenti riservate delle credenziali di autenticazione, deve essere effettuata considerando i seguenti elementi:

Sicurezza Nella Progettazione E Sviluppo Di Soluzioni Informatiche

- presenza di vincoli legislativi e/o regolamenti;
- livello di classificazione delle informazioni (ad es. in caso di informazioni "Riservate" o "Strettamente riservate", facendo riferimento alle indicazioni riportate all'interno del documento SIC-STD-06 *"Classificazione e gestione degli asset"*).

Nel caso in cui l'applicazione preveda anche il trattamento di dati sensibili occorre:

- prevedere che il salvataggio di dati su supporto elettronico avvenga utilizzando tecniche di cifratura oppure conservando i dati sensibili separatamente dai dati personali in modo da evitare accessi non autorizzati ad informazioni particolari;
- prevedere che il trasferimento di dati particolari sia eseguito con tecniche di cifratura per evitare il transito sulla rete degli stessi in chiaro.

2.1.1.6 Criteri per il tracciamento

Le applicazioni devono prevedere adeguate funzioni di tracciatura degli eventi rilevanti ai fini della sicurezza. I criteri da considerare in fase di progettazione sono i seguenti:

- progettare e prevedere l'impostazione delle applicazioni in modo tale da garantire il monitoraggio ed il tracciamento degli eventi di sicurezza correlati all'applicazione stessa, definendo gli eventi chiave per la sicurezza che devono essere tracciati e i tempi di retention dei relativi log, in conformità alle richieste provenienti dalle normative vigenti. Le informazioni da tracciare devono comprendere almeno i seguenti eventi:
  - accessi alle applicazioni avvenuti con successo;
  - tentativi di accesso alle applicazioni non completati con successo o non autorizzati;
  - attività di tipo amministrativo o associate ad accessi di tipo privilegiato: deve essere prevista almeno la registrazione degli access log così come richiesto dal Provvedimento del Garante per la protezione dei dati personali del 27/11/2008;
  - errori;
- prevedere meccanismi di autenticazione ed autorizzazione per il controllo degli accessi ai sistemi di generazione dei dati di tracciamento e ai dati stessi, al fine di garantire il corretto esercizio delle funzionalità di tracciatura e prevenire la modifica o la cancellazione non autorizzata dei dati di log;
- prevedere, dove possibile, l'invio dei log verso repository esterni (ad es. syslog).

2.1.1.7 Criteri per l'architettura applicativa

Relativamente all'architettura applicativa occorre definire i seguenti elementi:

- specifiche di prestazione;
- specifiche di integrazione relative a:
  - interfaccia nei riguardi di sistemi/servizi già esistenti, con la definizione delle loro caratteristiche e criteri;

  - individuazione degli archivi (compresi i database), delle procedure di controllo, dei programmi che devono essere adattati e di eventuali strumenti da predisporre;
- specifiche legate all'architettura di rete da impiegare, ai criteri di segregazione dell'applicazione da altre reti nonché – per applicazioni distribuite – legate all'organizzazione dell'applicazione su più reti;
- meccanismi di sicurezza (es. firma elettronica) tali da garantire il non ripudio delle transazioni là dove occorre fornire idonee garanzie di avvenuta spedizione/ricezione di determinati flussi telematici.

2.1.2 Requisiti per la progettazione di una componente infrastrutturale

Di seguito sono riportate le linee guida di sicurezza e/o misure/specifiche legate alla progettazione di una componente infrastrutturale ovvero alla predisposizione delle componenti hardware, software di base e middleware dell'infrastruttura tecnologica necessaria per l'erogazione del servizio:

- le tecnologie utilizzate devono essere, per quanto possibile, note e scelte in funzione del know-how presente all'interno di Trentino Digitale;
- la componente infrastrutturale da implementare deve soddisfare adeguati livelli di sicurezza in materia di business continuity e disaster recovery, che ricadono su elementi quali ad esempio:
  - livelli di ridondanza (minimizzazione degli SPOF);
  - capacità di ripristino da errori/fallimenti del sistema;
  - distribuzione dei componenti, se possibile, su siti differenti;
- devono essere definite soluzioni in grado di garantire la sicurezza fisica degli apparati e delle reti, prestando particolare attenzione alle modalità di cablaggio (elettrico e di trasporto dati), alla collocazione delle apparecchiature e alla presenza di gruppi di continuità elettrica;
- devono essere garantiti adeguati livelli di modularità al fine di garantire i requisiti di flessibilità e scalabilità della soluzione;
- la disponibilità di elementi di protezione contro il rischio di intrusione (adozione di opportune difese perimetrali, es. firewall);
- devono essere effettuate attività di hardening prima che gli apparati in questione siano connessi alla rete;
- il dimensionamento dei sistemi (es. memoria, processori, spazio disco occupato, traffico di rete, ecc.) deve essere effettuato in maniera tale da prevenire anomalie o malfunzionamenti determinati da sovraccarichi (*rif.* SGQ-PR-35.1 "*Capacity Management*"). In particolare, occorre:
  - stabilire quali soluzioni e quali funzioni sottoporre a misurazione;
  - definire e documentare un processo di raccolta dei dati e definizione dei parametri di accettabilità relativi ai livelli di prestazione;
  - definire e documentare un processo di analisi delle prestazioni.
- ogni componente architetturale (es. web server, application server, firewall, reverse proxy, intrusion detection etc.) prevista deve:

- essere attestata su una piattaforma sulla quale è stata condotta un'attività di hardening (eliminazione dei servizi/utility non necessari) e comunque priva di vulnerabilità note (installazione di patch);
- essere oggetto di un'attività di vulnerability assessment, effettuata secondo le specifiche valide nell'ambito di riferimento;
- prevedere, ove possibile, operazioni di tracciatura dell'accesso utenti secondo le specifiche valide nell'ambito di riferimento.

2.1.2.1 Ulteriori criteri per le LAN

Per mantenere un adeguato livello di sicurezza, nella progettazione delle LAN devono essere rispettati i seguenti principi:

- deve essere prevista una idonea segmentazione della lan aziendale in modo da realizzare zone di sicurezza con diversi livelli di protezione (es. lan client, lan server etc.);
- devono essere definiti dei controlli specifici per la salvaguardia dell'integrità e della confidenzialità dei dati critici in transito, in particolare su reti wireless;
- devono essere previsti meccanismi per garantire la registrazione degli eventi a meno che non possibile per limiti tecnologici degli apparati proprietari;
- devono essere definite opportune soluzioni tecniche di sicurezza per il controllo delle connessioni basate su meccanismi di riconoscimento degli indirizzi di rete del richiedente e del destinatario (es. firewall, NAC).

2.1.3 Requisiti per la predisposizione di altre componenti non informatiche

L'attività di predisposizione di un servizio è finalizzata anche a progettare e predisporre le componenti non informatiche necessarie per l'erogazione del servizio. Nel corso di tale attività occorre tenere in considerazione le seguenti specifiche, con riguardo alla sicurezza:

- le eventuali normative che possono avere impatto sul servizio, e i relativi adempimenti connessi ad esse (es. servizi per i quali occorre prevedere la pubblicazione di una informativa, come previsto dal D.Lgs. 196/03);
- le necessarie misure di disponibilità dei dati trattati, in termini di RTO ed RPO, in funzione delle esigenze di affidabilità e continuità del servizio, ivi compresa la l'eventuale stagionalità di queste ultime;
- la definizione delle modalità di inoltro di eventuali richieste di modifiche e/o accesso al servizio, ivi compresa la definizione dell'elenco dei richiedenti autorizzati (rif. SGQ-PR-50.3 "*Access Mangement*");
- le misure da implementare in caso di dismissione del servizio:
  - la modalità di richiesta della dismissione del servizio o di una sua parte;

- la politica e le modalità di ritenzione dei dati e/o del software e/o delle configurazioni dei sistemi, coerentemente con la natura dei dati trattati e la normativa in vigore;
- il servizio da predisporre per garantire eventuali accessi ai dati successivi alla dismissione dell'applicazione;
- l'eventuale eliminazione delle copie di back-up non più necessarie;
- le procedure da seguire per un corretto smaltimento degli asset coinvolti (rif. SIC-STD-06 "*Classificazione e gestione degli asset*", se non specificato diversamente dal Cliente e comunque sempre nel rispetto della normativa vigente);
- il processo di rimozione degli accessi e delle abilitazioni;
- eventuali comunicazioni verso terze parti o interne (ad esempio per l'aggiornamento dell'inventario, rif. SGQ-PR-90.1 "*Service Catalogue management*").

2.2 Progettazione di dettaglio, sviluppo e avviamento soluzione

La fase ha l'obiettivo di progettare nel dettaglio, realizzare e rendere disponibili le componenti applicative, di servizio e tecnologiche, scelte in funzione delle indicazioni fornite dall'Enterprise Architecture aziendale e/o del know-how presente all'interno di Trentino Digitale, necessarie per soddisfare i requisiti del progetto definiti nella precedente fase.

Di seguito sono riportate le linee guida di sicurezza associate alle macro-attività in cui si può scomporre questa fase:

- progettazione di dettaglio;
- sviluppo;
- esternalizzazione della produzione;
- verifica e validazione;
- installazione e avviamento della soluzione;
- validazione da parte del cliente.

2.2.1 Progettazione di dettaglio

Obiettivo della progettazione di dettaglio è recepire i requisiti o specifiche progettuali (specifiche infrastrutturali, specifiche funzionali e dell'architettura applicativa, specifiche di gestione del servizio, specifiche in termini di sicurezza - in ossequio al principio di "Privacy by design" previsto dalla normativa vigente), dell'applicazione qualora questa sia destinata alla gestione di dati personali) espressi nella precedente fase e tradurli in direttive tecniche ed operative.

2.2.1.1 Criteri per la progettazione di dettaglio di una componente applicativa

Qualora ritenuto opportuno, sulla base delle specificità del progetto ed eventualmente sulla base delle indicazioni della struttura responsabile della progettazione e della struttura responsabile della gestione

della sicurezza delle informazioni, nel caso di progettazione di dettaglio di software occorre considerare anche i seguenti ulteriori elementi:

- individuazione delle potenziali minacce e vulnerabilità (Threat Modeling) che possono mettere in pericolo la sicurezza dell'applicazione tramite un'analisi degli scenari chiave di utilizzo dell'applicazione e l'identificazione delle risorse critiche per le quali è necessario garantire particolare protezione;
- definizione delle metodologie e dei meccanismi di sicurezza da utilizzare sulla base delle vulnerabilità rilevate nel corso dell'attività di Threat Modeling (per i dettagli in merito alle principali minacce e relative contromisure fare riferimento al documento SIC-LG-06 *"Sviluppo sicuro: principali minacce e relative contromisure"*).

2.2.2 Sviluppo

2.2.2.1 Criteri per lo sviluppo di una componente applicativa

Durante lo sviluppo di una soluzione applicativa, ivi compresa la predisposizione delle procedure e della documentazione necessaria ad assicurarne la piena operatività, occorre tenere presente i seguenti criteri:

- le attività di sviluppo devono garantire l'aderenza alle best practice nazionali e internazionali in merito alla progettazione sicura del software (ad esempio quelle per lo sviluppo sicuro del codice);
- le attività di sviluppo delle applicazioni devono essere effettuate in un ambiente informatico distinto da quello di produzione, allineato allo stesso in termini di release e aggiornamenti;
- i dati utilizzati negli ambienti di sviluppo devono essere, là dove possibile, diversi da quelli di produzione e comunque epurati da ogni dato personale reale;
- devono essere implementati i requisiti di sicurezza definiti e validati nella fase di analisi;
- devono essere utilizzate specifiche soluzioni in grado di garantire l'integrità e la tracciabilità delle diverse versioni e modifiche del software (es. tramite piattaforme di gestione del versioning) nonché della relativa documentazione (*Configuration Management*), considerando, là dove possibile, i seguenti criteri:
    - evitare di mantenere su sistemi di produzione le librerie sorgenti dei programmi;
    - effettuare il controllo degli accessi a tali librerie, tracciando le attività effettuate;
    - mantenere i programmi oggetto di sviluppo e manutenzione separati dalle librerie di sorgenti di programmi che sono attivi in produzione;
    - definire delle procedure per effettuare copie di sorgenti, oltre che per il loro utilizzo, stabilendo le responsabilità, i livelli autorizzativi necessari e le procedure operative;
    - assicurare che i sistemi sui quali le copie sono ripristinate garantiscano lo stesso livello di protezione dei sistemi originali;
- si devono proteggere i sorgenti dei programmi assegnando specifiche responsabilità per la loro gestione, in modo tale da garantire che non siano effettuati accessi non autorizzati;

- si devono definire appropriate procedure di gestione delle librerie dei sorgenti
- deve essere definita una procedura di autenticazione che non permetta l'accesso alle applicazioni in fase di sviluppo per gli utenti non in possesso di idonee credenziali di autenticazione;
- deve essere predisposta la documentazione di rilascio;
- deve essere predisposta la manualistica utente (formazione) ed i documenti operativi di gestione per chi dovrà prendersi in carico la soluzione;
- devono essere adottate e rispettate le procedure formali per garantire il passaggio "sicuro" tra diversi ambienti (ad esempio il passaggio tra l'ambiente di sviluppo e l'ambiente di produzione).

2.2.3 Esternalizzazione della Produzione

In caso di esternalizzazione della produzione occorre seguire, nella gestione delle terze parti coinvolte/nella selezione del fornitore e del prodotto, delle specifiche linee guida di sicurezza.

2.2.3.1 Criteri per lo sviluppo di una componente applicativa in outsourcing

Sono valide tutte le linee guida fornite in precedenza, le quali vanno opportunamente inserite e descritte all'interno del rapporto contrattuale.

Occorre inoltre definire e formalizzare, sempre a livello contrattuale, adeguati controlli per garantire, anche in termini di sicurezza, la qualità del software sviluppato. A tal proposito si faccia riferimento alla policy SIC-POL-04 *"Aspetti contrattuali connessi con la sicurezza delle informazioni"*.

2.2.3.2 Criteri per l'acquisizione di pacchetti software sul mercato

Occorre definire apposite modalità di acquisizione di pacchetti applicativi da terzi. Pertanto, le linee guida da seguire sono:

- si deve verificare che il prodotto acquisito rispetti i requisiti di sicurezza dichiarati, quelli richiesti e quelli necessari per l'installazione e gestione del prodotto;
- si deve utilizzare il software applicativo protetto da copyright in base alle disposizioni fissate dai relativi contratti di concessione di licenza. In particolare, non si devono apportare modifiche al software acquisito, ad eccezione delle necessarie configurazioni e personalizzazioni, che comunque devono essere effettuate secondo le modalità previste dal fornitore;
- si devono sempre conservare in luoghi sicuri le copie "master" del software acquisito;
- si deve considerare, durante la scelta del fornitore del software, anche la capacità di fornire supporto nel lungo periodo.