TRENTINO DIGITALE S.P.A.

Sicurezza nella progettazione e sviluppo di soluzioni informatiche

1 PRINCIPALI MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE

Data	Versione	Modifiche apportate
	01.00 Obsoleta	Prima emissione
	01.01 Obsoleta	Integrazione dei riferimenti alle procedure ITIL del SGQ e dei requisiti inerenti alla dismissione di un servizio coerentemente con la progettazione di un servizio in ottica ITIL; 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.
	02.00 Obsoleta	Modifiche a seguito dell'aggiornamento della norma ISO27001
	02.01 Obsoleta	Modifica dei riferimenti all'SGQ in seguito della variazione degli stessi.
	03.00 Obsoleta	Adeguamento a seguito del nuovo asset aziendale e dell'entrata in vigore della nuova normativa relativa alla gestione dei dati personali
19/09/2019	04.00 In vigore	Aggiornamento template documento

INDICE

1 Introduzione

1.1 Premessa

Obiettivo del presente documento è fornire i principi che devono essere adottati per integrare gli aspetti di sicurezza delle informazioni in tutte le fasi legate alla progettazione e allo sviluppo di soluzioni informatiche, descritte all'interno del documento SGQ-LG-00 *"Progettazione e sviluppo – Modello di riferimento"*.

Con l'espressione "soluzioni informatiche" viene fatto riferimento ai prodotti/servizi erogati e in particolare:

- software applicativo e le relative infrastrutture tecnologiche (software di base e di ambiente, sistemi elaborativi e reti di telecomunicazione) sulle quali dovrà operare (per i dettagli relativi allo sviluppo fare riferimento al documento SGQ-PR-07 *"Sviluppo di software applicativo e system integration"*);
- infrastrutture tecnologiche a supporto dell'erogazione dei servizi informatici previsti (per i dettagli relativi alla progettazione e sviluppo fare riferimento al documento SGQ-PR-10 *"Progettazione e sviluppo di sistemi e reti"*);
- servizi informatici, spesso da erogare con il supporto di specifici software applicativi e/o infrastrutture tecnologiche (per i dettagli relativi alla progettazione e sviluppo fare riferimento al documento SGQ-PR-22.1 *"Progettazione e sviluppo di servizi informatici"*).

La progettazione e lo sviluppo di una nuova soluzione informatica costituisce uno sforzo complesso, limitato nel tempo, intrapreso per raggiungere obiettivi specifici, denominato progetto.

L'erogazione di servizi informatici comporta, invece, lo svolgimento, con continuità nel tempo, delle attività previste in sede di progettazione del servizio stesso (gestione, controllo, monitoraggio e misurazione). Le misure di sicurezza riferite al processo di erogazione non sono oggetto del presente documento ma trattate nella policy aziendale SIC-POL-10 *"Sicurezza nell'esercizio e gestione di soluzioni informatiche"*.

1.2 Perimetro organizzativo

La presente policy si applica a tutto il personale dipendente di Trentino Digitale e a tutti i soggetti che collaborano con Trentino Digitale.

1.3 Termini e definizioni

- *Asset o Bene* – Qualsiasi risorsa che abbia un valore per l'organizzazione, sia essa materiale o immateriale (es. beni fisici, software, informazioni e dati...).
- *Autenticità* – Proprietà per la quale è garantito che l'identità di un soggetto o di una risorsa è quella dichiarata; l'autenticità si applica ad entità quali utenti, processi, sistemi ed informazioni (ISO/IEC 13335-1:2004).
- *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.
- *Disponibilità* – Proprietà per la quale le informazioni sono rese accessibili ed utilizzabili su richiesta di un'entità autorizzata (ISO/IEC 13335-1:2004).
- *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.
- *Integrità* – Proprietà per la quale l'accuratezza e la completezza degli asset è salvaguardata (ISO/IEC 13335-1:2004).
- *Non ripudio* – Capacità di dimostrare che un'azione o un evento hanno avuto luogo, in modo che questo evento od azione non possano essere ripudiati successivamente (ISO/IEC 13335-1:2004).
- *Riservatezza* – Proprietà per la quale le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati (ISO/IEC 13335-1:2004).
- *Servizio informatico* – 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.
- *Trattamento* - 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.
- *Violazione* – la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- *Vulnerabilità* – Debolezza intrinseca di un componente del sistema informativo aziendale 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” Provvedimento del Garante privacy del 27/11/2008, pubblicato in G.U. n. 300 del 24 dicembre 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” Provvedimento a carattere generale del 17 gennaio 2008 *“Sicurezza dei dati di traffico telefonico e telematico”* del Garante per la Protezione dei Dati Personali
Standard di Riferimento	UNI CEI ISO/IEC 27001:2014 “Tecnologie Informatiche – Tecniche per la Sicurezza – SGSI - Requisiti” 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-LG-07 “Sicurezza delle informazioni nella progettazione e sviluppo di soluzioni informatiche” SIC-POL-04 “Aspetti contrattuali connessi con la sicurezza delle informazioni” SIC-POL-09 “Change Management” SIC-POL-10 “Sicurezza nell’esercizio e gestione di soluzioni informatiche”
A documenti del Sistema di Gestione della Qualità	SGQ-LG-00 “Progettazione e sviluppo – Modello di riferimento” SGQ-PR-22.3 “Progettazione e sviluppo di servizi informatici” SGQ-PR-22.2 “Progettazione e realizzazione di componente di un progetto” SGQ-PR-10 “Progettazione e sviluppo di sistemi e reti” SGQ-PR-30.1 “Service Level Management” SGQ-PR-50.2 “Request fulfilment”

	SGQ-PR-80.1 “Release and deployment Management”

2 Policy

Le soluzioni informatiche devono essere progettate e sviluppate in modo da garantire la loro massima efficienza ed efficacia ed un livello di sicurezza coerente con le informazioni trattate. Pertanto, occorre tenere in considerazione i seguenti requisiti generali:

- deve essere tenuta in considerazione la necessità di preservare la riservatezza, l’integrità e la disponibilità delle informazioni gestite;
- deve essere assicurata la disponibilità di capacità e di risorse adeguate a ottenere le prestazioni richieste;
- devono essere mantenuti, per quanto possibile, separati gli ambienti utilizzati (sviluppo, test, produzione) nelle varie fasi del ciclo di vita;
- tutte le applicazioni sviluppate devono rispondere alle previsioni legislative e normative vigenti, con particolare attenzione a quanto richiesto dal D.lgs. 196/03 concernente la protezione dei dati personali, nonché dal Provvedimento del Garante privacy del 27/11/2008 (“*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008”*) e dal Provvedimento del 17 gennaio 2008 (“*Sicurezza dei dati di traffico telefonico e telematico*”);
- nello sviluppo di applicazioni, dove ritenuto necessario sulla base delle specificità di progetto ed eventualmente sulla base delle indicazioni della struttura responsabile della gestione della sicurezza delle informazioni, valutare l’applicazione delle contromisure riportare nel documento SIC-LG-06 “*Sviluppo sicuro: principali minacce e relative contromisure*”;
- nello sviluppo di applicazioni, nel caso in cui si utilizzi software di terze parti, occorre affidarsi solo a fornitori che presentino idonee caratteristiche. Per i criteri che devono essere adottati in fase di selezione dei fornitori occorre fare riferimento al documento SIC-POL-04 “*Aspetti contrattuali connessi con la sicurezza delle informazioni*”;
- tutte le clausole contrattuali disciplinanti il rapporto con le terze parti (committente, fornitori) devono essere note, rispettate e monitorate nell’ambito della conduzione delle diverse attività (riferimento al documento SIC-POL-04 *“Aspetti contrattuali connessi con la sicurezza delle informazioni”*);
- deve essere prestata attenzione alla formalizzazione e alla completezza della documentazione;
- occorre verificare la necessità di prevedere un’adeguata formazione del personale coinvolto nella progettazione e nello sviluppo di una nuova soluzione informatica.

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 e successivamente definire la proposta di soluzione che li soddisfi tutti.

Nell'ambito dell'attività di formalizzazione dei requisiti occorre prestare attenzione ai seguenti aspetti:

- i requisiti devono essere formalizzati in un documento evidenziando gli aspetti funzionali, architetturali, di sicurezza ecc... Nel documento devono essere riportati anche gli eventuali rischi di sicurezza derivanti dall'implementazione delle soluzioni necessarie per rispondere alle esigenze espresse dal cliente e, nel caso sia previsto il trattamento di dati personali, l'eventuale impatto che una violazione potrebbe avere nei confronti degli interessati. Sui requisiti di sicurezza è necessario ottenere il parere del Responsabile per la Protezione dei Dati;
- i requisiti devono comprendere e considerare gli aspetti legati alla normativa vigente, e in particolare le esigenze in materia di protezione, controllo e verifica dei dati, dei processi elaborativi e delle attività in cui si scompone il servizio che si sta sviluppando. Qualora il cliente non li esprima formalmente, è compito di Trentino Digitale esplicitarli per favorire la definizione delle specifiche;
- in fase di definizione dei requisiti di una nuova soluzione informatica e in fase di verifica della proposta deve essere coinvolta la struttura preposta alla gestione della sicurezza delle informazioni, al fine di garantire un supporto per la corretta interpretazione e applicazione della normativa vigente e delle policy aziendali (per le evolutive il suo coinvolgimento deve essere valutato di volta in volta, identificando i casi per i quali si possono avere impatti sulla sicurezza della soluzione);
- la richiesta di introduzione di nuovi elementi in ambienti già esistenti deve essere chiaramente definita e sottoposta ad attenta analisi per valutare gli eventuali rischi di sicurezza associati.
- In termini generali, nell'ambito dell'attività di individuazione dei requisiti occorre prendere in considerazione almeno i seguenti ambiti:
- gli aspetti di sicurezza fisica (se applicabili);
- l'aderenza allo standard UNI CEI ISO/IEC 27001:2014 (se applicabile);
- i diversi profili di utenza (es. amministratore dell'applicazione, operatore, ospite) da prevedere in modo da poter associare un ruolo specifico ad ogni utente che viene creato;
- la tipologia di dati che verranno trattati (disaggregati, personali e/o identificativi, particolari) in modo da poter correttamente valutare le misure minime di sicurezza da applicare, ai sensi della normativa vigente e delle procedure aziendali;
- i flussi di dati (in particolare da/verso l'interfaccia utente e da/verso altri sistemi eventualmente coinvolti);
- la disponibilità dei dati trattati da garantire in accordo con i requisiti espressi dal cliente e comunque, in caso di trattamento di dati personali, conforme a quanto previsto dal D.lgs. 196/03 e dal Regolamento (UE) 2016/679;

- eventuali aspetti di sicurezza per le componenti "non informatiche" necessarie per l'erogazione del servizio;
- eventuali aspetti di sicurezza da definire per la dismissione del servizio;
- per la progettazione di una componente applicativa:
    - sistema di autenticazione e autorizzazione degli utenti e/o delle entità (es. processi inter-applicativi e batch);
    - gestione delle attività degli utenti;
    - validazione dei dati in Input/Output;
    - utilizzo di Meccanismi Crittografici;
    - tracciatura degli eventi rilevanti ai fini della sicurezza;
- per la progettazione di una componente infrastrutturale:
    - tracciatura degli eventi rilevanti ai fini della sicurezza;
    - aspetti di business continuity e disaster recovery;
    - integrità e confidenzialità dei dati critici in transito sulle reti pubbliche;
    - controllo e registrazione degli accessi;
    - collocazione degli apparati all'interno dell'infrastruttura di telecomunicazioni esistente.

Per maggiori dettagli fare riferimento a quanto riportato all'interno del documento SIC-LG-07 "*Sicurezza delle informazioni nella progettazione e sviluppo di soluzioni informatiche*".

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, tecnologiche e di servizio 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, espressi nella precedente fase e tradurli in direttive tecniche ed operative.

L'output di tale attività deve essere validato dalla struttura responsabile della progettazione e dalla struttura preposta alla gestione della sicurezza delle informazioni, al fine di garantire un supporto per la corretta interpretazione e applicazione della normativa vigente e delle policy aziendali (per le evolutive il

coinvolgimento di quest'ultima deve essere valutato di volta in volta, identificando i casi per i quali si possono avere impatti sulla sicurezza del servizio).

Nel caso la progettazione riguardi una soluzione software occorre individuare le potenziali minacce e vulnerabilità che possono mettere in pericolo la sicurezza dell'applicazione, tramite un'analisi degli scenari chiave di utilizzo e l'identificazione delle risorse critiche per le quali è necessario garantire particolare protezione, definendo successivamente le metodologie ed i meccanismi di sicurezza da utilizzare sulla base delle vulnerabilità rilevate (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

- L'attività di sviluppo delle componenti informatiche deve:
- essere condotta solo a seguito di una formale accettazione delle specifiche definite in fase di progettazione;
- devono essere implementati i requisiti di sicurezza definiti e validati nella fase di analisi;
- ispirarsi alle principali best practices in materia di *sviluppo sicuro del software*;
- essere effettuata in un ambiente informatico distinto da quello di produzione, allineato allo stesso in termini di release e aggiornamenti, contenente dati, là dove possibile, diversi da quelli di produzione e comunque epurati da ogni dato personale;
- implementare una gestione degli accessi degli utenti agli ambienti di sviluppo coerente con i dati trattati;
- prevedere la predisposizione della manualistica utente (formazione) e dei documenti operativi di gestione per chi dovrà prendersi in carico la soluzione, nonché tutta la documentazione necessaria per il rilascio;
- prevedere appropriate procedure e/o soluzioni in grado di garantire l'integrità e la tracciabilità delle diverse versioni e modifiche del software nonché della relativa documentazione (Configuration Management).

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 (per i criteri che devono essere adottati in fase di selezione dei fornitori occorre fare riferimento al documento SIC-POL-04 "*Aspetti contrattuali connessi con la sicurezza delle informazioni*").

Sia in caso di sviluppo di una componente applicativa in outsourcing, sia in caso di acquisizione di pacchetti software sul mercato, restano 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, opportune clausole con le terze parti per garantire, anche in termini di sicurezza, la qualità del software acquisito; tali clausole devono

essere rispettate e monitorate nell'ambito delle diverse attività (riferimento al documento SIC-POL-04 *"Aspetti contrattuali connessi con la sicurezza delle informazioni"*).

2.2.4 Verifica e validazione

La verifica e la successiva validazione degli aspetti di sicurezza di un progetto è finalizzata ad accertarsi che siano soddisfatti i requisiti e le condizioni imposte durante tutta la progettazione. I test devono riguardare anche le caratteristiche di sicurezza e la verifica di eventuali vulnerabilità applicative.

Nell'ambito di questa fase occorre inoltre rispettare le indicazioni di seguito riportate:

- le modalità per effettuare le verifiche ed i controlli, l'analisi dei risultati e la loro approvazione devono essere formalizzate;
- tutte le verifiche ed i controlli effettuati, nonché i relativi esiti, devono essere documentati;
- devono essere implementati e tracciati tutti gli interventi correttivi emersi a fronte delle anomalie rilevate;
- si devono verificare, tra gli altri, i seguenti aspetti:
    - il rispetto di tutti i requisiti funzionali e di sicurezza identificati durante tutta la durata del progetto;
    - le prestazioni effettuate, in condizioni simulate o reali, del servizio prodotto;
    - la corretta configurazione dell'infrastruttura tecnologica a supporto della soluzione informatica (hardening).
- le attività di testing delle funzionalità delle applicazioni devono essere condotte:
    - sulla base di una pianificazione formale ed utilizzando apposite checklist;
    - in un ambiente separato ma allineato, in termini di contromisure di sicurezza, a quello di produzione;
    - ponendo particolare attenzione alla profilatura e ai diritti di accesso degli utenti;
    - utilizzando dati coerenti con quelli di produzione;
    - qualora ritenuto opportuno, sulla base delle specificità del progetto ed eventualmente sulla base delle indicazioni della struttura responsabile della gestione della Sicurezza delle Informazioni o del Responsabile per la Protezione dei Dati, occorre verificare la robustezza dell'applicazione simulando un attacco in ambiente di test *(penetration test applicativo*) e/o eseguire un'analisi statica dell'applicazione (*code review*) attraverso metodi manuali ed automatici di verifica dei codici sorgente dell'applicazione con il fine di individuare codice non conforme alle linee guida/requisiti definiti;
- nell'ambito dei test devono essere effettuate delle verifiche di performance, volte a verificare la capacità dell'intera soluzione di sopportare picchi di utilizzo sia in termini di attività contemporanee degli utenti, che in termini di mole di dati trattati.

2.2.5 Installazione e avviamento soluzione

L'attività è finalizzata a rendere operative, dopo la formale approvazione e accettazione delle strutture responsabili, le soluzioni predisposte negli step precedenti, comprendendo dunque l'avviamento del servizio (lo start-up infrastruttura tecnologica, l'installazione e l'avviamento della soluzione applicativa).

Relativamente alla gestione del passaggio in produzione devono essere rispettati i seguenti criteri (rif. SGQ-PR-80.1 "*Release and deployment Management*"):

- l'attività di rilascio deve essere attentamente e formalmente pianificata; in particolare, deve essere prevista una specifica presa in carico del servizio;
- prima di procedere ai rilasci, occorre (rif. SGQ-PR-50.2 "*Request fulfilment*"):
    - verificare la presenza di un back-up dei dati consistente;
    - predisporre e pianificare tutte le procedure di restore in caso di problemi conseguenti all'attività;
    - predisporre un tracciamento e monitoraggio intensificato dei nuovi sistemi in produzione per un periodo di tempo opportuno (rif. SGQ-PR-30.1 "Service Level Management");
    - predisporre adeguati piani formativi per gli operatori al fine di consentire il corretto utilizzo dei sistemi.
- prima di procedere all'avviamento dei servizi, occorre verificare che tutta la documentazione a corredo dei servizi sia completa e coerente. In particolare, occorre che siano state predisposte opportune procedure per:
    - il monitoraggio del sistema e l'analisi dei relativi log;
    - la verifica dei dati relativi alle prestazioni delle diverse componenti del servizio;
    - la gestione delle credenziali di autenticazione e dei profili di accesso degli utenti;
    - il salvataggio dei dati secondo le modalità stabilite;
    - la gestione delle attività di assistenza.

2.2.6 Validazione da Parte del Cliente

Obiettivo di tale attività è fornire il necessario supporto per lo svolgimento del collaudo da parte del cliente per l'accettazione della soluzione informatica prodotta, ivi compreso il collaudo dei relativi aspetti di sicurezza.

2.3 Variazioni in condizioni di esercizio

A fronte di esigenze di modifica emerse in fase di progettazione e sviluppo occorre garantire che esse siano gestite in modo opportuno e secondo procedure predisposte ad hoc in modo tale da minimizzare i rischi di sicurezza: per le linee guida relative alle modalità di gestione dei change fare riferimento al documento SIC-POL-09 "Change Management".

3 Definizione dei ruoli e delle responsabilità

3.1 Strutture responsabili della progettazione e sviluppo dei servizi

Le strutture aziendali preposte alla progettazione dei servizi hanno la responsabilità principale di eseguire le attività di definizione dei requisiti e pianificazione, coerentemente con quanto riportato all'interno della presente policy (par. 2.1).

Tali strutture hanno inoltre la responsabilità di coordinare le attività di progettazione di dettaglio, sviluppo e avviamento, di validare i risultati delle altre strutture.

È inoltre compito di tali strutture, in caso di progettazione di una nuova soluzione informatica, coinvolgere la struttura preposta alla gestione della sicurezza delle informazioni al fine di garantire un supporto per la corretta interpretazione e applicazione della normativa vigente e delle policy aziendali (per le evolutive il suo coinvolgimento deve essere valutato di volta in volta, identificando i casi per i quali si possono avere impatti sulla sicurezza della soluzione) e del Responsabile per la Protezione dei Dati al fine di verificare l'adozione di misure di sicurezza adeguate relativamente ai dati personali.

3.2 Strutture responsabili della gestione dei servizi

Le strutture aziendali preposte alla gestione dei servizi hanno la responsabilità della formale approvazione e accettazione e di fornire supporto in fase di collaudo e di attivazione dei servizi, coerentemente con quanto riportato all'interno della presente policy (par. 2.2.4 e 2.2.5).

3.3 Strutture responsabili della progettazione e realizzazione delle componenti applicative

Le strutture aziendali deputate alla gestione e al coordinamento delle attività di progettazione e realizzazione delle componenti applicative hanno la responsabilità, coerentemente con quanto riportato all'interno della presente policy (par. 2.2.1, 2.2.2 e 2.2.3), di:

- redigere le specifiche progettuali, tecniche, funzionali, di sicurezza e relative alla gestione del servizio, in coerenza con i requisiti espressi;
- realizzare e sviluppare gli applicativi nel rispetto delle best practices in materia di sicurezza e delle disposizioni aziendali;
- garantire il passaggio tra ambienti (test, sviluppo, quality e produzione) nel rispetto delle regole di cui alla presente policy;
- condurre test puntuali e che tengano debitamente conto anche degli aspetti di sicurezza;
- redigere tutta la documentazione di supporto.

In caso di esternalizzazione della produzione le medesime strutture sono responsabili di gestire i rapporti con i fornitori e di far eseguire quanto sopra specificato, secondo linee guida opportunamente inserite e descritte all'interno del rapporto contrattuale.

3.4 Strutture responsabili della gestione del data center

Le strutture aziendali responsabili della gestione del data center hanno la responsabilità di garantire le attività di predisposizione dell'infrastruttura tecnologica coerentemente con quanto riportato all'interno della presente policy.

3.5 Struttura Responsabile della Gestione della Sicurezza delle Informazioni

La struttura responsabile della gestione della sicurezza delle informazioni deve fornire supporto in relazione all'interpretazione e applicazione della normativa e delle policy aziendali, alla redazione dei requisiti di sicurezza nella progettazione di nuovi servizi.