TRENTINO DIGITALE S.P.A.

Sicurezza nell'esercizio e gestione di soluzioni informatiche

PRINCIPALI MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE

Data	Versione	Modifiche apportate
	01.0 Obsoleta	Prima emissione
	01.1 Obsoleta	Integrazione principi generali per la gestione degli accessi alla rete a seguito della dismissione del corrispondente documento dedicato e dei riferimenti alle procedure ITIL del SGQ ed eliminazione riferimenti SGQ-PR-11 soppressa.
	02.0 Obsoleta	Modifiche a seguito dell'aggiornamento della norma ISO27001
	03.0 Obsoleta	Adeguamento a seguito del nuovo asset aziendale e alla normativa di riferimento in vigore relativa Protezione delle persone fisiche con riguardo al trattamento dei dati personali
19/09/2019	04.0 Obsoleta	Aggiornamento template documento
16/10/2020	04.1 In Vigore	Inserimento riferimenti al Cloud pubblico

INDICE

1 Introduzione 4
1.1 Premessa 4
1.2 Perimetro organizzativo 4
1.3 Termini e definizioni 4
1.4 Riferimenti 7
2 Policy 9
2.1 Principi generali 9
2.2 Gestione operativa 9
2.3 Gestione dei cambiamenti 12
2.4 Monitoraggio e verifiche 12
2.4.1 Monitoraggio e tracciamento 12
2.4.2 Verifiche tecniche 13
3 Ruoli e responsabilità 14
3.1 Strutture responsabili della gestione del data center 14
3.2 Strutture responsabili della gestione delle applicazioni 14
3.3 Strutture preposte alla gestione del servizio 14
3.4 Struttura responsabile della gestione della sicurezza delle informazioni 15
3.5 Struttura responsabile della protezione dei dati (DPO) 15

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 in tutte le fasi legate all'esercizio e alla gestione di soluzioni informatiche, come previsto anche dallo standard UNI CEI ISO/IEC 27001:2014.

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

- Software applicativo e relative infrastrutture tecnologiche (software di base e di ambiente, sistemi elaborativi e reti di telecomunicazione) sulle quali questo dovrà operare;
- Infrastrutture tecnologiche, a supporto dell'erogazione dei servizi informatici previsti;
- Servizi informatici, da erogare con il supporto di specifici software applicativi e/o infrastrutture tecnologiche.

L'esercizio e la gestione di soluzioni informatiche comporta lo svolgimento con continuità nel tempo delle attività previste in sede di progettazione, e quindi riguarda le modalità di gestione, controllo, monitoraggio e misurazione messe in atto (per quanto riguarda invece le misure di sicurezza riferite al processo di progettazione e sviluppo fare riferimento al documento SIC-POL-08 "Sicurezza nella progettazione e sviluppo di soluzioni informatiche").

1.2 Perimetro organizzativo

La presente policy si applica a tutte le soluzioni informatiche in esercizio e conseguentemente a tutto il personale dipendente e ai collaboratori, che operano per conto di Trentino Digitale, deputati alla loro gestione.

1.3 Termini e definizioni

Amministratore di Sistema – Con questa espressione viene fatto riferimento alle figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché alle figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Antivirus – Software atto a rilevare ed eliminare virus informatici o, più in generale, malware.

CED – Centro Elaborazione Dati.

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.

Sicurezza Nell'esercizio E Gestione Di Soluzioni Informatiche

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

DMZ (Demilitarized Zone) - Letteralmente "Zona Demilitarizzata", indica un'area della rete che, pur trovandosi all'interno del dominio protetto da un firewall necessita di livelli di protezione maggiori rispetto a quelli applicati alle LAN di utilizzo generale.

DNS (Domain Name Server) - Sistema utilizzato per la risoluzione di nomi di host in indirizzi IP e viceversa.

Hardening – Insieme di azioni atte ad analizzare le funzionalità di un sistema operativo/applicazione al fine di individuare la configurazione ottima che permetta di innalzare il livello di sicurezza e ridurre il rischio residuo connesso alle debolezze dei sistemi.

Host – Il termine host viene usato nell'ambito delle connessioni in rete per definire i nodi di rete, intesi come elaboratori, che svolgono e ospitano qualche tipo di servizio.

Firewall - Dispositivo hardware e/o software, solitamente connesso nei punti di contatto tra reti diverse per disciplinare il traffico in transito secondo un set di regole prestabilito e configurato al suo interno. Solitamente un firewall protegge le reti interne da Internet ma può anche essere utilizzato per proteggere reti interne ad alta sensibilità dalla rete degli utenti locale dal traffico di informazioni che transita da e verso reti esterne, in particolar modo Internet.

IaaS – (Infrastructure-as-a-Service) Infrastruttura erogata in modalità di servizio. Risorse hardware virtualizzate vengono messe a disposizione, affinché l'utilizzatore possa creare e gestire, secondo le proprie esigenze, una propria infrastruttura sul cloud senza preoccuparsi di dove siano allocate le risorse

IDS – L'Intrusion Detection System è una piattaforma tecnologica avente l'obiettivo di analizzare a fondo il traffico in transito (generalmente autorizzato da un firewall) con l'obiettivo di rilevare potenziali attacchi camuffati al suo interno.

Malware – È un qualunque software creato con lo scopo di causare danni sul computer su cui viene attivato e/o eseguito. Il termine deriva dalla contrazione delle parole inglesi malicious e software che in italiano è equivalente a "codice maligno".

Monitoraggio - Il complesso di operazioni effettuate per controllare lo stato dell'infrastruttura ICT e dei servizi applicativi.

Patching - Una patch (denominata anche "fix") è la riparazione di una parte dei programmi informatici che mostrano instabilità e/o problemi connessi con la sicurezza. Spesso temporanea, in vista dell'integrazione nella versione successiva dei programmi, una patch sistema i problemi (chiamati anche "bug") riscontrati in un determinato programma durante la sua esecuzione. Una patch è la soluzione immediata fornita agli utenti da parte dei produttori di software. Quasi sempre può essere scaricata dai siti internet dei produttori stessi.

Sicurezza Nell'esercizio E Gestione Di Soluzioni Informatiche

Server – Un qualunque sistema di elaborazione connesso in rete che fornisce servizi ad altri componenti informatici e su cui sia stato installato un Sistema Operativo specificamente destinato ad utilizzo "server".

Time Server – Soluzione che garantisce la sincronizzazione dell'orologio interno di tutte le piattaforme tecnologiche attraverso l'utilizzo di un protocollo standard.

Tracciamento - Insieme di azioni volte a raccogliere ed elaborare i dati (log) prodotti dal monitoraggio e dai sistemi informatici e finalizzate alla rilevazione di eventi anomali e incidenti di sicurezza.

Utente finale – Colui che usufruisce di un bene o di un servizio.

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.

Virus – Software che ha il solo scopo di danneggiare i sistemi che lo ospitano. Un virus, per entrare in funzione, deve essere eseguito, più o meno intenzionalmente, la prima volta.

Worm – Particolare forma di malware che, a differenza di un virus, è in grado di replicare sé stesso autonomamente.

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"*
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"

Sicurezza Nell'esercizio E Gestione Di Soluzioni Informatiche

A documenti del Sistema Sicurezza	• SIC-LG-04 *"Regolamento sul corretto utilizzo delle risorse aziendali - Dipendenti"* • SIC-LG-07 *"Sicurezza nella progettazione e sviluppo di soluzioni informatiche"* • SIC-POL-04 *"Aspetti contrattuali connessi con la sicurezza delle informazioni"* • SIC-POL-05*"Identificazione, classificazione e gestione degli asset"* • SIC-POL-08 *"Sicurezza nella progettazione e sviluppo di soluzioni informatiche"* • SIC-POL-09 *"Change Management"* • SIC-POL-13 – "*Politica di sicurezza per i servizi in Cloud Pubblico*"; • SIC-PR-03 *"Gestione del ciclo di vita delle utenze"* • SIC-IO-04 *"Gestione del back-up e della movimentazione dei dati, della conservazione e del reimpiego dei supporti di memorizzazione"* • SIC-IO-08 *"Gestione accessi fisici"* • SIC-STD-08 *"Norme per la raccolta e la conservazione dei* • *log"* • SIC-STD-10 *"Predisposizione sistemi antivirus"* • SIC-STD-19 "*Accesso alla rete di Trentino Digitale*"
A documenti del Sistema di Gestione della Qualità	• SGQ-PR-40.1 "*Event Management*" • SGQ-PR-30.1 "*Service Level Management*"

2 Policy

2.1 Principi generali

Le soluzioni informatiche devono essere gestite in modo da garantire il mantenimento di adeguati livelli di efficienza e da preservare al meglio le informazioni che vengono trattate per il loro tramite. Pertanto, occorre tenere in considerazione i seguenti requisiti generali:

- le soluzioni informatiche in produzione devono essere gestite mantenendo i livelli di sicurezza previsti da Trentino Digitale;
- per tutti i servizi erogati, devono essere garantite le attività di assistenza previste dal Sistema di Gestione della Qualità aziendale;
- devono essere adottate adeguate metodologie e strumenti idonei al controllo ed al monitoraggio della soluzione informatica, compresi i livelli di sicurezza (rif. SGQ-PR-30.1 “Service Level Management”);
- a fronte delle informazioni raccolte nel corso delle attività di assistenza e monitoraggio/tracciamento, tramite anche l’esecuzione di analisi periodiche, devono essere definite le eventuali esigenze di intervento (criticità e vulnerabilità) e stabilite in via conseguente le opportune azioni correttive e preventive per il miglioramento, o il mantenimento, dei livelli di efficienza/efficacia della soluzione informatica;
- la dismissione delle soluzioni informatiche deve essere gestita in modo sicuro:
  - rispettando l’iter di autorizzazione aziendale;
  - verificando la presenza di eventuali vincoli di natura contrattuale;
  - definendo puntualmente un piano di disattivazione;
  - garantendo, se necessario, tutte le adeguate comunicazioni verso le terze parti;
  - garantendo un corretto smaltimento e riutilizzo degli asset della soluzione informatica da dismettere, prevedendo la cancellazione dei dati trattati e la rimozione del software installato (i metodi di cancellazione adottati devono essere coerenti, in termini di livelli di sicurezza garantiti, con i livelli di criticità delle informazioni gestite).

2.2 Gestione operativa

La sicurezza delle informazioni si realizza ponendo attenzione agli aspetti connessi alla gestione operativa di sistemi, reti, applicazioni e in generale di servizi, in modo da assicurare il loro funzionamento corretto e sicuro nel tempo.

Tutte le attività attinenti alla gestione in esercizio di una soluzione informatica, sia questa allocata nei datacenter aziendali o su Cloud Pubblico, devono essere infatti condotte nel rispetto di una serie di regole di sicurezza coerenti con le principali best practice nazionali e internazionali.

In particolare, è necessario individuare opportune modalità operative almeno per le seguenti attività:

- avvio e arresto delle soluzioni informatiche e delle relative componenti;
- schedulazione di eventuali job (compresi i requisiti e le eventuali interdipendenze con altre piattaforme);
- manutenzione ordinaria e straordinaria (incluso l’aggiornamento delle piattaforme);
- salvataggi delle informazioni e loro gestione;

- registrazione (logging) e monitoraggio degli eventi (rif. SGQ-PR-40.1 “Event Management”);
- gestione di errori o altre condizioni anomale;
- riavvio e ripristino delle soluzioni informatiche e delle operazioni;
- implementazione di specifici automatismi di verifica e controllo sulla correttezza delle operazioni.

Nell’ambito della gestione operativa delle soluzioni informatiche occorre inoltre prestare attenzione ai seguenti requisiti:

- deve essere mantenuta, ove possibile, la separazione degli ambienti (sviluppo, collaudo, produzione) nei quali i sistemi, le applicazioni e in generale i servizi devono essere installati, gestiti e mantenuti;
- deve essere adeguatamente mantenuta aggiornata e protetta la documentazione di sistema (es. configurazioni, procedure operative) al fine di garantire un corretto svolgimento delle attività;
- devono essere adottate opportune procedure per garantire la manutenzione delle piattaforme, in osservanza con le specifiche fornite dai vendor;
- le soluzioni informatiche devono essere protette da accessi non autorizzati in modo adeguato rispetto la loro criticità;
- tutti gli asset necessari per l’erogazione di una soluzione informatica devono essere registrati nell’asset database aziendale così come definito anche all’interno del documento SIC-POL-05 “Identificazione, classificazione e gestione degli asset”;
- devono essere adottate opportune misure di sicurezza per la protezione dei sorgenti del software prodotto in azienda;
- occorre prevedere un apposito processo per le attività di patching che tenga conto della frequenza degli aggiornamenti e delle modalità di validazione delle patch rilasciate;
- nel caso la fase di esercizio sia gestita, anche parzialmente, in outsourcing, devono essere definite specifiche misure di protezione (es. opportune clausole contrattuali, verifiche periodiche), secondo le linee guida riportate all’interno del documento SIC-POL-04 “Aspetti contrattuali connessi con la sicurezza delle informazioni”;
- nel caso la soluzione sia allocata all’interno di un Cloud Pubblico, devono essere definite specifiche misure di protezione (es. opportune clausole contrattuali, verifiche periodiche), secondo le linee guida riportate all’interno del SIC-POL-13 – “Politica di sicurezza per i servizi in Cloud Pubblico”;
- è necessario provvedere alla rimozione di tutte le informazioni ad Uso Interno, Riservate o Strettamente Riservate (vedi SIC-POL-05 “Identificazione, classificazione e gestione degli asset” per le definizioni) prima di trasportare una risorsa al di fuori dell’azienda per attività di assistenza e riparazione;
- l’utilizzo di supporti informatici removibili deve essere limitato ai soli casi strettamente necessari per la corretta conduzione dell’attività aziendale;
- le componenti fisiche (server, apparati di rete, ...) facenti parte delle soluzioni informatiche, devono essere posizionati in aree il cui accesso è controllato e può essere limitato ai soli

Sicurezza Nell'esercizio E Gestione Di Soluzioni Informatiche

amministratori di sistema, come definito all'interno del documento SIC-IO-08 "Gestione accessi fisici";

- l'accesso sistemistico alle componenti delle soluzioni informatiche, da un qualunque punto esterno alla rete di Trentino Digitale, deve essere fornito soltanto tramite l'utilizzo di una VPN, secondo le modalità previste dalla SIC-STD-19 "Accesso alla rete di Trentino Digitale";
- il controllo e la gestione degli accessi logici deve essere allineato alle normative vigenti in materia e alle disposizioni aziendali (per ulteriori dettagli fare riferimento a quanto riportato all'interno del documento SIC-PR-03 "Gestione del ciclo di vita delle utenze" e del documento SIC-LG-04 "Regolamento sul corretto utilizzo delle risorse aziendali - Dipendenti");
- deve essere garantita la sincronizzazione dell'orario di sistema di tutte le piattaforme tecnologiche con i time server aziendali qualora tecnicamente possibile. Nel caso le piattaforme tecnologiche siano allocate su Cloud di tipo pubblico, è necessario richiedere puntualmente al fornitore su quale tipo di time server viene sincronizzata la sua infrastruttura;
- l'accesso alle risorse facenti parte della soluzione informatica, deve essere inibito manualmente se lasciate incustodite. Dove tecnicamente fattibile devono essere previste funzionalità di blocco dell'accesso ad attivazione automatica dopo al massimo 10 minuti di inattività;
- prima di connettere un server alla rete di produzione di Trentino Digitale, deve essere effettuato il collaudo secondo quanto previsto dalla policy SIC-POL-08 "Sicurezza nella Progettazione e Sviluppo di soluzioni informatiche". In tale sede deve essere verificata anche l'aderenza del sistema in analisi alle policy di sicurezza da parte della struttura responsabile della gestione della sicurezza delle informazioni;
- nella pianificazione delle attività di upgrade a nuove versioni devono essere definite le procedure per il ripristino della versione precedente sicuramente funzionante (roll back);
- si devono controllare periodicamente le prestazioni delle soluzioni informatiche gestite (memoria, processori, spazio disco occupato, traffico di rete, ecc.), operando delle proiezioni sulle necessità future delle risorse, sulla base dei risultati delle analisi prestazionali condotte e delle evoluzioni che possono interessare l'intero sistema informativo dell'Azienda e comunicando eventuali decadimenti delle prestazioni, al fine di adottare delle opportune azioni correttive per il miglioramento delle performance.
- devono essere attivate delle procedure e implementate specifiche contromisure tecniche e organizzative per la rilevazione e prevenzione della diffusione di malware informativi nelle soluzioni informatiche (per ulteriori dettagli fare riferimento a quanto riportato all'interno del documento SIC-STD-10 "Predisposizione sistemi antivirus" e SIC-LG-04 "Regolamento sul corretto utilizzo delle risorse aziendali - Dipendenti");
- si deve prevedere una corretta e completa attività di backup dei dati, con modalità documentate e collaudate.
- I dettagli relativi alle modalità di gestione dei back-up sono disponibili nel documento SIC-IO-04 "Gestione del back-up e della movimentazione dei dati, della conservazione e del reimpiego dei supporti di memorizzazione")

- i server che espongono servizi verso l'esterno (Internet o Intranet PAT) devono essere collocati nelle DMZ aziendali. Inoltre, tali server devono essere associati a un proprio Domain Name Server (DNS) record.
- Nel garantire agli utenti autorizzati l'accesso ai sistemi e alla rete dell'Azienda devono essere rispettati i seguenti requisiti:
  - stabilire delle modalità di connessione differenziate a seconda della tipologia di utente che si collega (dipendente, personale esterno, utente nomadico)
  - separare gli ambienti informatici a seconda delle loro finalità (sviluppo, test/integrazione, produzione);
  - segregare la rete al fine di individuare i "punti di contatto" critici tra reti interne, reti periferiche e reti esterne. Tali punti di contatto devono essere sempre controllati e monitorati tramite appositi strumenti quali firewall, IDS/IPS, ecc.;
  - utilizzare opportuni meccanismi di autenticazione e autorizzazione degli utenti. Qualora le esigenze di sicurezza lo richiedano è opportuno prevedere meccanismi di autenticazione forte;
  - utilizzare meccanismi di comprovata affidabilità qualora sia previsto il passaggio di dati su reti esterne o wireless;
  - istituire segmenti di rete dedicati, per il personale esterno che deve operare all'interno dell'azienda, per limitare eventuali conseguenze di accessi non autorizzati o utilizzi abusivi delle risorse.

Nel documento SIC-STD-19 "Accesso alla rete di Trentino Digitale" sono descritte le modalità specifiche di accesso alla rete di Trentino Digitale per ognuna delle seguenti situazioni:

- accesso alla rete dalle sedi di Trentino Digitale;
- accesso alla rete da remoto.

2.3 Gestione dei cambiamenti

Tutte le modifiche devono essere gestite in modo opportuno secondo le procedure predisposte al fine di garantire la correttezza degli interventi minimizzando i rischi, i disservizi, gli effetti sulla continuità operativa e i costi: per le linee guida relative alle modalità di gestione dei change fare riferimento al documento SIC-POL-09 "Change Management".

2.4 Monitoraggio e verifiche

2.4.1 Monitoraggio e tracciamento

Al fine di garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi, nonché di assicurare la sicurezza e la disponibilità delle soluzioni informatiche gestite e delle relative informazioni, deve essere predisposto un processo di monitoraggio avente l'obiettivo di rilevare situazioni anomale, accessi non autorizzati, indicazioni sull'utilizzo e sullo stato dell'infrastruttura ICT e dei servizi applicativi etc...

Qualora l'evento anomalo rilevato interessi dati personali, deve essere immediatamente informato il Responsabile della protezione dei dati (DPO), affinché valuti la gravità della violazione e, se del caso,

provveda ad inviare la prevista comunicazione all'autorità Garante e agli Interessati. Dell'evento deve inoltre essere informato il Titolare del trattamento e il Comitato Privacy.

La raccolta ed elaborazione dei dati (log) prodotti dal monitoraggio e dai sistemi informatici devono essere predisposte rispettando i requisiti previsti dal documento SIC-STD-08 "Norme per la raccolta e la conservazione dei log".

2.4.2 Verifiche tecniche

Al fine di garantire adeguati livelli di sicurezza e affidabilità delle soluzioni informatiche devono essere condotte delle attività periodiche di verifica che ne certifichino lo stato. Tali attività devono essere effettuate anche in conseguenza di mutamenti significativi all'interno dell'Azienda (es. ridisegno dei sistemi di protezione, revisione organizzativa, evoluzione dell'architettura, ecc.).

In particolare, nell'ambito delle verifiche tecniche di sicurezza occorre prevedere:

- una fase di pianificazione, in cui individuare il perimetro di analisi, definire le finalità dell'attività e gli obiettivi che devono essere raggiunti, definire la periodicità dell'analisi (funzione della criticità, della complessità e dell'estensione dell'oggetto di verifica), preparare e sottoscrivere la documentazione legale (rilascio autorizzazioni, manleva), informare il personale coinvolto;
- una fase di esecuzione, che comporta la rilevazione delle vulnerabilità mediante analisi perimetrali e/o interne, eseguite in modo intrusivo o non intrusivo, condotte da società specializzate esterne con il supporto e la supervisione di risorse interne (o da eventuali risorse esterne sotto la propria responsabilità);
- una fase di analisi dei risultati, nella quale, sulla base dei dati raccolti nella fase precedente, vengono estratte le informazioni significative per individuare, in termini di gravità, le vulnerabilità e le criticità rilevate. Vengono inoltre proposte e discusse con le persone interessate tutte le misure di contrasto tecnologiche e/o organizzative ritenute necessarie per mitigare o eliminare le problematiche individuate;
- nel caso la vulnerabilità rilevata possa compromettere la corretta erogazione di uno dei servizi IaaS, la sua presenza e la sua gestione deve essere comunicata ai clienti interessati;
- una fase di produzione di reportistica e comunicazione dei risultati, nella quale viene preparata la relativa documentazione e vengono comunicati alle strutture interessate gli esiti dell'analisi;
- una fase di approvazione e implementazione delle contromisure, in cui sono approvate e predisposte eventuali azioni preventive e correttive per eliminare o mitigare l'esposizione alle vulnerabilità rilevate.

3 Ruoli e responsabilità

3.1 Strutture responsabili della gestione delle infrastrutture tecnologiche

Le strutture aziendali coinvolte nelle attività di esercizio e gestione delle infrastrutture tecnologiche e, in particolare, nella gestione del Data Center, hanno la responsabilità, coerentemente con quanto riportato all'interno della presente policy, di:

- garantire le attività di gestione utenze e controllo accessi;
- garantire la gestione sicura della rete;
- garantire la gestione sicura dei server;
- condurre attività di monitoraggio dell'utilizzo delle infrastrutture;
- condurre verifiche tecniche periodiche;
- garantire il rispetto delle attività di Configuration e Capacity Management;
- controllare periodicamente le prestazioni dei sistemi;
- assicurare la conduzione delle attività di back-up e l'esecuzione di verifiche periodiche in materia;
- garantire l'applicazione delle regole per la prevenzione del software dannoso;
- garantire la correttezza delle attività di dismissione/riutilizzo delle componenti delle soluzioni informatiche.

3.2 Strutture responsabili della gestione delle applicazioni

Le strutture aziendali coinvolte nelle attività di esercizio e gestione delle soluzioni informatiche, e in particolare nella gestione delle componenti applicative delle stesse, hanno la responsabilità, coerentemente con quanto riportato all'interno della presente policy, di:

- garantire le attività di gestione utenze e controllo accessi;
- condurre attività di monitoraggio applicativo dell'uso delle soluzioni informatiche;
- condurre verifiche tecniche periodiche;
- garantire il rispetto delle attività di Configuration e Capacity Management;
- assicurare la conduzione delle proprie attività negli ambienti distinti di preproduzione e produzione;
- supportare le altre strutture nell'ambito dello sviluppo di nuove soluzioni;
- garantire la correttezza delle attività di dismissione/riutilizzo di soluzioni informatiche.

3.3 Strutture preposte alla gestione dei servizi

Le strutture aziendali coinvolte nelle attività di gestione dei servizi hanno la responsabilità, coerentemente con quanto riportato all'interno della presente policy, di:

- garantire le attività di assistenza;
- garantire la conduzione di attività di controllo e monitoraggio dei livelli di efficienza del servizio;
- garantire la conduzione di attività di backup e ripristino;
- garantire la separazione degli ambienti di preproduzione e produzione;

- attuare tutti gli interventi preventivi e correttivi ritenuti necessari a fronte dei risultati delle attività di assistenza e monitoraggio.

3.4 Struttura responsabile della gestione della sicurezza delle informazioni

La struttura responsabile della gestione della sicurezza delle informazioni ha le seguenti responsabilità:

- supportare le altre strutture, nell'ambito della gestione delle soluzioni, nella definizione di opportune contromisure sulla base delle risultanze dell'analisi dei rischi;
- ricevere e gestire rapporti periodici sulle potenziali situazioni di pericolo;
- collaborare alla predisposizione di piani formativi per il personale e per gli amministratori dei sistemi di sicurezza.

3.5 Struttura responsabile della protezione dei dati (DPO)

La struttura responsabile della protezione dei dati, per lo scopo di questa procedura, ha le seguenti responsabilità:

- informare e fornire consulenza al titolare, al responsabile del trattamento e ai dipendenti sulla normativa in materia di protezione dei dati personali, inclusa quella nazionale applicabile;
- costituire il punto di contatto con il Garante, in relazione a ogni questione relativa al trattamento e la violazione dei dati personali;
- effettuare audit periodici sulle tempistiche e sulle modalità di trattamento dei dati personali al fine di verificarne l'aderenza alla normativa.