S.A.P. NA.

Sistema Ambiente Provincia di Napoli S.p.A.

Procedura per il Trattamento dei Dati Personali e la Sicurezza Informatica

PO.11.2016

LEBOTTI MARIO
23.06.01 08:05:53
Firma Digitale
CN=LEBOTTI MARIO
C=IT
2.5.4.4=LEBOTTI
2.5.4.42=MARIO

	UNITA' ORGANIZZATIVA	FIRMA
Redatto da:	*Ufficio Affari Generali*	*Ing. M. Lebotti* _____
Approvato da:	*Amministratore Unico*	*Dott. G. Gargano* _____
Pubblicazione:	*Ufficio Affari Generali*	

REVISIONE	DATA	DESCRIZIONE
00 – I° emissione	Luglio 2016	Procedura operativa n. 11
01 – II° emissione	Maggio 2023	Aggiornamento normativo e tecnologico

GARGANO
GABRIELE
01.06.2023
08:17:03
GMT+02:00

INDICE

ALLEGATI

Allegato 1: Format- Dichiarazione di Riservatezza (DOC 1 DOC 2 DOC 3)

Allegato 2: Schema Help Desk Informatico aziendale

1. Premessa

1.1. Nota introduttiva

Con il Decreto Legge n. 5 del 9 febbraio 2012, convertito dalla legge n. 35 del 4 aprile 2012, che ha modificato alcune disposizioni in materia di misure minime di sicurezza, L'obbligo di adozione di un Documento Programmatico sulla Sicurezza dei dati personali (DPS)[1] è stato soppresso. E' stata inoltre abolita anche la precedente possibilità, alternativa, di rilasciare l'"autocertificazione" a cura del titolare nonché il c.d. "DPS semplificato" del 2011.

1.2. Necessità della procedura

La redazione di una procedura in materia di trattamento dati e sicurezza informatica, per motivi organizzativi e gestionali, assume importanza fondamentale ai fini della dichiarazione, da parte dell'Azienda, **della propria politica in materia di trattamento dei dati sensibili,** delle procedure che regolano la corretta adozione delle azioni che riguardano il trattamento dei dati personali, le misura di sicurezza adottate per i dati trattati, nonché l'ottemperanza degli obblighi di legge previsti. E' necessario sottolineare che i sopraelencati provvedimenti di modificazione alla Legge sulla privacy, **non sollevano le aziende ed i titolari dall'attuazione di tutti gli altri adempimenti previsti dalla normativa sulla protezione dei dati personali**, e le successive integrazioni e modificazioni, ad oggi vigenti.
L'ente che espleta il controllo sull'attuazione delle succitate previsioni normative è il garante per la Privacy www.garanteprivacy.it
Il presente documento oltre a definire le azioni procedurali per il trattamento dei dati personali e la sicurezza informatica per la S.A.P.NA. S.p.A., rappresenta presidio per la prevenzione dei reati di cui al Dlgs 231/2001, riscontrando altresì le indicazioni del PNA di cui alla L. 190/2012 in materia di anticorruzione.

2. Definizioni, Riferimenti a Norme e Leggi, Responsabilità

2.1. Definizioni

Al fine di agevolare la lettura e la comprensione del significato normativo delle disposizioni del presente documento, si riportano di seguito le definizioni, fornite dal Garante, dei termini utilizzati nel Codice e degli acronimi usati per la redazione della presente procedura:

- **"S.A.P.NA. S.p.A.":** la società Sistema Ambiente Provincia di Napoli per Azioni, interamente partecipata da Pubblica Amministrazione;
- **"CMN":** la Città Metropolitana di Napoli;
- **"ATO":** genericamente gli Ambiti Territoriali Ottimali Napoli 1, Napoli 2 e Napoli 3;
- **"EdA":** genericamente gli Enti d'Ambito degli ATO EdA Napoli 1, Napoli 2 e Napoli 3;
- **"sede operativa":** gli uffici della sede operativa ubicati in Via Ponte dei Francesi, 37/E – Napoli;
- **"garante":** l'Autorità Garante della Privacy;
- **"trattamento":** qualunque operazione o complesso di operazioni, effettuati con o senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- **"dato personale":** qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- **"dati sensibili":** i dati idonei a rivelare i dati personali, lo stato di salute, lo stato patrimoniale o giuridico, le convinzioni religiose, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, politico o sindacale nonché la vita sessuale;

[1] già previsto dal DLgs 30 giugno 2003 n. 196 (normativa sulla protezione dei dati personali, in sostituzione della L.676/95), il DPS era sussistente per tutte le imprese, lavoratori autonomi, enti o associazioni che trattano dati personali - anche sensibili, giudiziari o con strumenti elettronici.

- **"titolare":** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- **"responsabile":** la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;
- **"incaricati":** le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- **"interessato":** la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

2.2. Riferimenti a Norme e Leggi

La presente procedura fa riferimento a:

- Leggi della Repubblica Italiana;
- Legge n. 26 del 26.02.2010 e ss. mm. e ii.;
- Legge Legge Regionale 26 maggio 2016, n. 14 Regione Campania e ss. mm. e ii.
- Statuto Aziendale vigente alla data di pubblicazione del presente documento;
- Decreto Legislativo 30 giugno 2003 n. 196 e ss. mm. e ii.;
- Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e ss. mm. e ii.;
- Decreto Legge n. 5 del 9 febbraio 2012, convertito in legge n. 35 del 4 aprile 2012;
- Conversione in Legge n. 134 del 7 agosto 2012 del DL 22 giugno 2012, n. 83 Titolo II Misure urgenti per l'Agenda Digitale e la Trasparenza nella Pubblica Amministrazione;
- Codice dell'Amministrazione Digitale, D.Lgs. 7 marzo 2005, n.82 e successive integrazioni e modificazioni;
- Decreto legislativo 19 agosto 2016, n. 175 Testo unico in materia di società a partecipazione pubblica come integrato dal decreto legislativo 16 giugno 2017, n. 100;
- AGID Agenzia per l'Italia Digitale: indirizzi, regole tecniche, linee guida e metodologie progettuali in materia di tecnologie informatiche;
- Precetti normativi di carattere generale e del Dipartimento della Funzione Pubblica in materia di trattamento e tutela dati personali;
- Codice Etico aziendale S.A.P.NA. S.p.A.;
- Procedure e Regolamenti vigenti in S.A.P.NA. S.p.A.;
- Modello di Organizzazione e Gestione, Rev. 4 - Maggio 2023 S.A.P.NA. S.p.A.;
- Regolamento Organismo di Vigilanza S.A.P.NA. S.p.A.;
- Norme Vigenti in materia di Anticorruzione - Legge n. 190/2012 e ss.;
- Norme Vigenti in materia di Trasparenza - Dlgs 33/2013 e ss.;
- Delibere ANAC in materia di trasparenza ed anticorruzione;
- Piano Triennale per la Prevenzione della Corruzione e per la Trasparenza (PTPCT);
- Regolamento generale sulla protezione dei dati (GDPR, General Data Protection Regulation - Regolamento UE 2016/679), 24 maggio 2016;
- Decreto legislativo 10 agosto 2018, n. 101, disposizioni per l'adeguamento dell'ordinamento nazionale al nuovo regolamento UE 2016/679;
- Dlgs 25 maggio 2016, n. 97 *Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza*, correttivo della legge 6 novembre 2012, n. 190 e del decreto legislativo 14 marzo 2013, n. 33. [recepimento del FoIA Freedom of Information Act].
- Legge 4 agosto 2021, n. 109 recante *"Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale"* conversione del DL 14 giugno 2021, n. 82;
- D.L. 21/2022 convertito con modificazioni dalla L. 20 maggio 2022, n. 51- Capo II art. 29 *"Cybersicurezza delle reti, dei sistemi informativi e dei servizi informatici…."* diversificazione dei prodotti informatici in uso dalle

pubbliche amministrazioni al fine di prevenire pregiudizi alla sicurezza delle reti, dei sistemi informativi e dei servizi informatici.

2.3. Responsabilità, Azioni e Applicazione

Sono responsabili dell'applicazione del presente documento:

A. Il **Titolare** del trattamento dati di S.A.P.NA. S.p.A.;
B. Il **Responsabile** del trattamento dati preposto dal Titolare;
C. Gli **Addetti** che abitualmente/occasionalmente trattano dati di S.A.P.NA. S.p.A.

Con apposito atto o determinazione dell'Amministratore Unico della S.A.P..NA. S.p.A. è individuato il Titolare del Trattamento dati. Il Titolare a sua volta, con apposito atto scritto indicherà i Responsabili del trattamento.
Oltre alle istruzioni generali su come devono essere trattati i dati personali, ai soggetti incaricati vengono fornite, da parte del Titolare, istruzioni base "di default" afferenti:

a) alle procedure da seguire per la classificazione dei dati personali, al fine di distinguere quelli sensibili e giudiziari, osservando le specifiche cautele di trattamento che questo tipo di dati richiedono;
b) alle modalità da osservare per la custodia e l'archiviazione degli stessi e procedure per il salvataggio dei dati;
c) alle modalità di conservazione, aggiornamento e custodia delle "password" occorrenti per l'accesso ai PC, ai server ed al sistema di rete aziendale, nonché alle modalità di elaborazione dei dati in essi contenuti;
d) alle prescrizioni circa le precauzioni da adottare per non lasciare incustoditi e accessibili i PC o i server o qualsiasi altro strumento elettronico attivo, che sia destinatario di dati sensibili, mentre è in corso una sessione di lavoro;
e) alle procedure ed alle modalità di utilizzo degli strumenti e dei programmi atti a proteggere i sistemi informativi ed all'aggiornamento sulle relative misure di sicurezza;
f) alle modalità di utilizzo, custodia e archiviazione dei supporti rimovibili contenenti dati personali;
g) all'osservanza dell'obbligo di riservatezza (Vedi **Allegati DOC 1 – 2 - 3:** Format - Dichiarazione Riservatezza);

La presente procedura è applicata all'intera società S.A.P.NA. Sistema Ambiente Provincia di Napoli S.p.A. Piazza Matteotti, 1 – Napoli partita iva e codice fiscale 06520871218. Pertanto sono *soggetti incaricati* i Responsabili della Unità organizzative presso la SEDE Uffici e delle Unità Locali decentrate di SAPNA S.p.A. così individuate:

- Unità Locale NA/1 - Sede Legale della Società - Napoli - Piazza Matteotti 1 Cap 80133 c/o Palazzo Provincia di Napoli
- Unita' Locale n. NA/2 – Discarica "Masseria del Pozzo" - Giugliano in Campania (NA) - Via Santa Maria a Cubito, snc Cap 80014
- Unita' Locale n. NA/3 Discarica "Masseria Del Re" - Giugliano in Campania (NA) -Via Madonna di Pantano snc Cap 80014
- Unita' Locale n. NA/4 Discarica/Sito di Ponte Riccio - Giugliano in Campania (NA) - Trav. Ponte Riccio - Zona ASI snc Cap 80014
- Unita' Locale n. NA/5 Discarica/Sito di Settecainate - Giugliano in Campania (NA) - Via Grotta dell'Olmo snc Cap 80014
- Unita' Locale n. NA/6 Discarica/Sito di Caivano Pascarola - Caivano (NA) - Via Pascarola snc Cap 80023 - Zona Industriale ASI Caivano
- Unita' Locale n. NA/7 Discarica/Sito di Pantano Acerra - Acerra (NA) – Località Pantano di Acerra snc Cap 80011
- Unita' Locale n. NA/8 Stabilimento Industriale TMB di Giugliano per la tritovagliatura, trattamento e selezione dei rifiuti solidi urbani non pericolosi. Giugliano in Campania (NA) Circumvallazione Esterna snc Zona ASI Cap 80014
- Unita' Locale n. NA/9 Stabilimento Industriale TMB di Tufino per la tritovagliatura, trattamento e selezione dei rifiuti solidi urbani non pericolosi. Tufino (NA) Strada prov. per Visciano snc Cap 80030 Frazione Localita' Schiava
- Unita' Locale n. NA/10 Discarica di Chiaiano - Napoli (NA) Via Cupa del Cane snc Cap 80145 Frazione CHIAIANO
- Unita' Locale n. NA/11 Discarica di Terzigno - Terzigno (NA) – Località Pozzelle snc Cap 80040
- Unita' Locale n. NA/12 Uffici Amministrativi Sede Operativa - Napoli (NA) Via Ponte dei Francesi 37/E Cap 80146
- Unita' Locale n. NA/13 Discarica di Villaricca – Villaricca Napoli (NA) Località Masseria Riconta, Via Viaticale, snc Cap 80010
- Unità Locale n. NA/14 – Discarica di Paenzano 1 – Tufino (NA) – Strada Prov.le per Visciano snc – Cap 80030

- Unità Locale n. NA/15 – Discarica di Paenzano 2 – Tufino (NA) – Via Cupatelle, snc Frazione Schiava – Cap 80030
- Unità Locale n. NA/16 – Discarica di Pirucchi – Palma Campania (NA) – Località Balle 2 – Cap 80036
- Unità Locale n. NA/17 – Discariche ASI Giugliano – Masseria del Pozzo (NA) – Via Santa Maria a Cubito, snc – Cap 80014
- Unità Locale n. NA/19–Sito di stoccaggio di Giugliano–Taverna del Re Lotto E–Giugliano in Campania (NA)–Via Madonna del Pantano, snc Taverna del Re, Cap 80014
- Unità locale n. NA/20- Discariche Resit- Località Scafarea, snc 80014 Giugliano in Campania (NA).

3. Finalità

Il presente documento regolamenta, disciplina e norma, nel rispetto del DLgs 30 giugno 2003 n. 196 e ss. mm. e ii., **il trattamento e la sicurezza dei dati personali e/o sensibili che vengono processati dalla S.A.P.NA. S.p.A.,** nell'ambito dell'espletamento delle sue funzioni istituzionali, delineando il quadro delle misure di sicurezza organizzative, fisiche e logiche poste a tutela dei dati stessi, indicando le linee guida per la conservazione e la messa in sicurezza dei dati, siano essi contenuti nei supporti informatici che contenuti in formato cartaceo, utilizzati dalla S.A.P.NA. S.p.A.

Fermo restando quanto previsto dalla presente procedura, ogni incaricato (di cui al prec. Par. 2.3.), nello svolgimento delle proprie mansioni e/o nella gestione di casi particolari, anche non espressamente disciplinati, dovrà attenersi alle predette linee guida, curando che siano rispettati i diritti dei soggetti interessati ed evitare che un errato trattamento del dato possa determinare conseguenze dannose per l'azienda e/o i terzi.

Nel caso specifico di trattamento dei dati personali, ad esempio, l'indicazione generale è quella di utilizzare, per quanto possibile, strumenti automatizzati e solo per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti.

Nei successivi paragrafi sono illustrate le specifiche misure di sicurezza che vengono osservate per prevenire l'uso illecito o non corretto del dato personale, la perdita dello stesso, nonché l'accesso al dato non autorizzato.

Per quanto riguarda il diritto dell'interessato alla conoscenza dell'esistenza di propri dati personali trattati presso la S.A.P.NA. S.p.A. nonché di conoscerne il contenuto, l'origine e verificarne l'esattezza, questo può essere esercitato in qualunque momento ai sensi dell'art. 7 del Dlgs n. 196/2003 (cfr. Titolo II Dvo.). Ai sensi del medesimo articolo il soggetto ha il diritto di chiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, nonché di opporsi in ogni caso, per motivi legittimi, al loro trattamento. Le richieste vanno rivolte ed inviate alla S.A.P.NA. S.p.A.

Lo scopo del presente documento è, pertanto, anche quello di fornire uno strumento attraverso il quale si vuole avere evidenza della rispondenza generale dell'Azienda nei confronti del Decreto Legislativo196/2003 ed in particolare dell'allegato B – Disciplinare Tecnico, in materia di misure minime di sicurezza.

3.1. Elementi base

Vengono di seguito identificati i principali componenti oggetto di elaborazione delle misure di sicurezza indispensabili per il rispetto di quanto stabilito dalla Norma:

- l'elenco e la tipologia dei dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, la tipologia di protezione delle aree e dei locali, ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti di:
  - rischi che incombono sui dati;
  - misure per la prevenzione di eventi dannosi;
  - disciplina sulla protezione dei dati personali più rilevanti in rapporto alle attività; responsabilità derivanti dal trattamento/conservazione dati;
  - modalità per l'aggiornamento sulle misure minime.

3.2. Tipologia dei Dati trattati

La S.A.P.NA. S.p.A. attua le seguenti tipologie di trattamento:

a) Trattamento dei dati personali di tutti i dipendenti e dei collaboratori professionali – per questi ultimi incluso il regime di collaborazione coordinata e continuativa - necessari alla corretta gestione del rapporto di lavoro, alla reperibilità e alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali, o dati di natura bancaria. Se al trattamento di tali dati concorre una struttura esterna – come ad es. studio professionale e/o società di elaborazione paghe - alla stessa sarà richiesto di rilasciare una dichiarazione di conformità alle misure minime di sicurezza della sua struttura. Il trattamento dei dati personali dei dipendenti può comportare anche il trattamento di dati sensibili dei dipendenti stessi;

b) Trattamento dei dati personali di operatori economici e terzi ricavati da albi, elenchi pubblici, visure camerali oppure concernenti la corrispondenza con gli stessi, dati commerciali, nonché i dati necessari ai fini fiscali o i dati di natura bancaria per le operazioni di pagamento.

L**a tipologia dei dati trattati nell'ambito della SAP.NA. S.p.A.** è così individuata:

Per singoli soggetti, con riferimento al personale dipendente

- informazioni di carattere anagrafico;
- informazioni di carattere sanitario;
- informazioni sulle caratteristiche del nucleo familiare;
- informazioni sulle ore lavorate, straordinari, permessi, attività sindacali, etc.
- informazioni sulla retribuzione;
- informazioni relative agli estremi di conti correnti bancari o postali;
- informazioni di carattere previdenziale e assicurativo;
- informazioni su provvedimenti pignorativi sulla retribuzione;
- informazioni su provvedimenti coatti sulla retribuzione;
- informazioni di natura giudiziaria, civile o penale;

Per singoli soggetti, con riferimento a terzi, non dipendenti

- informazioni di carattere anagrafico;
- informazioni sulle caratteristiche e composizione del nucleo familiare;
- informazioni su partecipazioni societarie, cariche amministrative, etc.
- informazioni di natura professionale e commerciale;
- informazioni di natura giudiziaria, civile o penale;

Per società, con riferimento a Società commerciali e/o assimilati e/o Enti pubblici e/o assimilati

- informazioni di natura commerciale;
- contratti d'appalto per la Fornitura, Servizi e Lavori;
- preventivi per Forniture, Servizi e Lavori;
- documenti fiscali, fatture e corrispondenza clientela;
- informazioni relative agli estremi di conti correnti bancari o postali;
- atti di proprietà;
- atti patrimoniali e simili;
- visure e certificati catastali;
- atti costitutivi e modificativi di società;
- documentazione grafica e fotografica di beni immobili e mobili della propria clientela;
- informazioni di carattere penale sugli amministratori o componenti della società;
- informazioni di provvedimenti giudiziari di qualsiasi natura;
- informazioni sulla regolarità contributiva;
- informazioni sulla regolarità fiscale;
- informazioni su progetti, brevetti, marchi e processi;

Per società, con riferimento alla Società S.A.P.NA. S.p.A.

- informazioni di natura commerciale;
- contratti d'appalto per la Fornitura, Servizi e Lavori;
- preventivi per Forniture, Servizi e Lavori;

- documenti fiscali, fatture ricavi e fatture costi;
- informazioni relative alla corrispondenza in ingresso ed in uscita;
- estratti conto bancari;
- informazioni relative agli estremi di conti correnti bancari o postali;
- atti di proprietà;
- atti patrimoniali e simili;
- visure e certificati catastali;
- atti costitutivi e modificativi di società;
- documentazione grafica e fotografica di beni immobili e mobili della propria clientela;
- informazioni sugli amministratori o componenti della società;
- informazioni di carattere giudiziario di qualsiasi natura;
- informazioni sulla regolarità contributiva e assicurativa;
- informazioni sulla regolarità fiscale;
- informazioni su progetti, brevetti, marchi e processi;
- delibere delle Assemblee dei Soci;
- determinazioni dell'Organo Amministrativo;
- verbali del Collegio dei Sindaci;
- verbali dell'Organismo di Vigilanza.

3.3. Trattamento delle Informazioni - Compiti e Responsabilità

Fermo quanto previsto dalla presente procedura, ogni incaricato nello svolgimento delle proprie mansioni e comunque, nella gestione di casi particolari non espressamente disciplinati, dovrà attenersi alle indicazioni contenute nel presente documento, curando che, in ogni caso, siano rispettati i diritti dei soggetti interessati dal trattamento, conservazione e messa in sicurezza dei dati contenuti nei supporti informatici e/o cartacei, utilizzati dalla SAP.NA. S.p.A. ed evitare che il trattamento del dato possa determinare conseguenze dannose per l'azienda e/o i terzi. Pertanto, con riferimento alle attività previste al punto b) del par. 3.1, vengono identificate le principali operazioni che vengono effettuate, nell'ambito societario, di trattamento dell'informazione e del dato sensibile ad essa connesso. Atteso che, per quanto afferisce la presente procedura, sono considerati "sensibili" le tipologie dei dati di cui all'elenco del par. 3.2., limitatamente ed esclusivamente alla loro utilità per le azioni necessarie alle attività di S.A.P.NA. S.p.A., le operazioni effettuate su questi dati sono riassunte nelle seguenti fasi:

Fase 1:

- acquisizione e reperimento dei dati/informazioni, direttamente dalla persona interessata (soggetto fisico o giuridico), o presso terzi, ovvero indirettamente per il tramite di apposito accesso autorizzato a banche dati presso siti istituzionali (prefettura, agenzia delle entrate, tribunale, Inps, CCIAA, etc.) o a mezzo dichiarazione ex Art. 47 D.P.R. 28.12.2000, n. 445;

Fase 2:

- registrazione del dato/informazione acquisito, inserimento dello stesso in supporti informatici o cartacei, intendendo per supporto informatico oltre a supporto fisico anche l'allocazione in *Cloud* del dato;

Fase 3:

- uso del dato/informazione così registrato limitatamente all'ambito delle attività aziendali che lo richiedono;

Fase 4:

- intervento di modifica dei dati così registrati, in relazione a variazioni o nuove acquisizioni, limitatamente all'ambito delle attività aziendali che lo richiedono;

Fase 5:

- conservazione dei dati per tutto il tempo necessario agli scopi per i quali sono stati raccolti o successivamente trattati;

Fase 6:

- cancellazione, rimozione, restituzione o distruzione dei dati, quando sono terminati gli scopi per cui sono stati inizialmente raccolti o quando sono elassi i termini di legge per la conservazione del dato/documento.

Ciò premesso, le responsabilità ed i compiti per il trattamento dei dati nelle suddette fasi di processo, sono identificate da S.A.P.NA. S.p.A. nella tabella di seguito riportata (Tav.1) con la quale si individuano:

1) *il titolare del trattamento;*
2) *la tipologia dei dati e la finalità che viene perseguita;*
3) *gli strumenti utilizzati per il trattamento degli stessi;*
4) *l'eventuale intervento nel processo (e condivisione del dato) di enti esterni, come ad esempio ditte specializzate, studi professionali, esperti, etc.*

NOTA DI INDIRIZZO GENERALE

Tutti i documenti ricevuti e/o emessi dall'Azienda sono protocollati e conservati secondo i criteri di Legge stabiliti dal Codice dell'Amministrazione Digitale per il tramite di apposito software omologato.

S.A.P.NA. S.p.A. ottempera agli obblighi di produrre in digitale la documentazione aziendale ai sensi dell'articolo 40 del Codice dell'Amministrazione Digitale. Essa in quanto società interamente partecipata da Pubblica Amministrazione alla quale è soggetta per coordinamento e controllo, aderisce ed osserva le regole tecniche di cui al DPCM 13.11.2014 in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici. Pertanto qualsiasi dato che sia inserito o faccia parte di documenti comunque sottoposti a processo di archiviazione, e quindi protocollati dall'Azienda, sono sempre conservati in un archivio telematico "cloud" esterno alla società, sottoforma di file scansionato, reso protetto, archiviato, e disponibile presso la conservatoria.

La protocollazione e la successiva archiviazione/conservazione avviene per il tramite di specifico software (c.d. FOLIUM) in uso ai dipendenti dell'Azienda, abilitati a loro volta in esclusiva per determinati accessi e in ragione del grado/livello di riservatezza e classificazione del documento, sia di consultazione che di operazione.

Per i particolari in dettaglio si veda la Procedura PO 07.2014 e ss. mm. e ii "Gestione Documentazione Sede Operativa, Flusso Protocollo e Distribuzione Posta".

Nella tabella 1 seguente sono riassunte le aree aziendali con la rispettiva tipologia dei dati principalmente trattati e la finalità che il trattamento consegue, gli strumenti utilizzati per il trattamento e la eventuale condivisione del dato

Tabella. 1

Area aziendale che opera il trattamento	**Tipologia dei Dati Trattati e finalità**	**Strumenti utilizzati**	**Eventuali condivisioni del Dato**
Gare e Contratti	Archivio ed anagrafica clienti e fornitori, contratti e archivio contratti Dati su operatori economici derivanti da gare d'appalto, da gare CONSIP, da gare MePA, etc. Dati derivanti da consultazioni INPS, Equitalia, Casellario Giudiziale, CCIAA, Prefettura, Tribunali	Personal computer e documentazione cartacea, posta elettronica certificata, sistema protocollazione aziendale, fax, scanner, stampanti locali e remote, collegamenti telematici Firma digitale dell'Amministratore.	- Consulenze e/o assistenza Legale in convenzione in materia di Appalti - DIGITAL PA per la manutenzione periodica piattaforma dell'Albo Fornitori e del Sito web istituzionale
Amministrazione e Finanza	Archivio ed anagrafica clienti e fornitori per flussi finanziari, dati concernenti pagamenti e bonifici compreso IBAN, consultazione Banche, istituti di credito; Dati derivanti da consultazioni INPS ed Equitalia, Agenzia delle Entrate, agenzia delle Entrate Riscossione; Dati derivanti da documenti contabili e fiscali; Archivio documenti fiscali e contabili; Archivio dei Verbali del collegio dei sindaci;	Personal computer e documentazione cartacea, posta elettronica certificata, sistema protocollazione aziendale, fax, scanner, stampanti locali e remote, collegamenti telematici Software contabilità certificati Firma digitale dell'Amministratore	- STUDIO IMPRESA per la sola attività specialistica Fiscale e Tributaria - DEDA Group per la conservazione sostitutiva dei dati di fatturazione elettronica su cloud esterno DEDA NEXT SRL Società Unipersonale

Amministrazione del Personale	Archivio ed anagrafica di: personale dipendente e personale in collaborazione. Archivio curriculum vitae dei dipendenti, schede personali dei dipendenti. Cartelle sanitarie dei dipendenti. Archivio rilevazione presenze personale dipendente, straordinari, assenze, permessi, etc. Archivio dei cedolini paga dei dipendenti e dei collaboratori con cedolino paga Dati derivanti da consultazioni INPS, INAIL, etc. Dati derivanti da fidi, cessioni quinto stipendio, garanzie e pignoramenti nei confronti di dipendenti Archivio versamenti contributivi e fiscali per i dipendenti. Archivio CUD lavoratori dipendenti. Archivio contenzioso in materia di lavoro.	Personal computer e documentazione cartacea, sistema protocollazione aziendale, posta elettronica, fax, scanner, stampanti locali e remote, collegamenti telematici Software cedolini paghe Software Zucchetti di elaborazione paghe Software rilevamento presenze NET-TIME Software Zucchetti per consultazione cedolino paga rilevazione presenze a mezzo biometrico-dati conservati dal dipendente sul proprio badge	- Italia Paghe Srl Inclusa attività di assistenza Fiscale (mod. 770 ademp. fisc., DM10 Etc.) per il personale dipendente
Affari Generali	-Archivio, anagrafica e parcelle di avvocati professionisti esterni. Archivio anagrafica da contratti con i Comuni. -Archivio anagrafica e curriculum vitae di tutti i professionisti esterni. -Archivio dei procedimenti in giudizio non di lavoro. Pignoramenti di terzi nei confronti dell'azienda. Procure speciali da Notaio.	Personal computer e documentazione cartacea, posta elettronica, sistema protocollazione aziendale, fax, scanner, stampanti locali e remote, collegamenti telematici	Occasionalmente e di volta in volta in caso di affidamento della controversia ad avvocato
	Archivio Libri Determinazioni dell'Amministratore Unico. Archivio Libri Deliberazioni dell'assemblea del socio unico. Archivio delle disposizioni Organizzative. Archivio delle Determinazioni dirigenziali. Archivio dei Verbali dell'Organismo di Vigilanza. Archivio delle Procedure Organizzative e dei Regolamenti aziendali. Trasmissione delle determinazioni e delle disposizioni organizzative. Raccolta dati economici e gestionali relativi al controllo interno	Personal computer e documentazione cartacea, posta elettronica ordinaria, sistema protocollazione aziendale, fax, scanner, stampanti locali e remote, collegamenti telematici	Nessun ausilio esterno
Direzione Tecnica	Gestione dei dati relativi a comunicazioni e documentazioni relative a rapporti con Enti Società ed Imprese, inerenti i diversi settori dell'Ufficio Tecnico, con particolare riferimento alle attività di fornitura, servizi e lavori. Qualsiasi elaborato di progetto e dati in essi contenuti. Dati economici e commerciali da ricerche di mercato e da gare. Archivio e Gestione dei dati relativi ad analisi e monitoraggi ambientali. Archivio degli elaborati di progetto, dei disciplinari tecnici e dei documenti sulla sicurezza. Dati afferenti i professionisti e/o commissioni di gara esterne. Archivio dei dati afferenti il flusso e la quantità dei rifiuti entranti ed uscenti dagli impianti prima e dopo il trattamento meccanico. Sistemi di videosorveglianza, centrale di acquisizione immagini per scopi di sorveglianza e prevenzione furti, esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, nel rispetto delle altre garanzie previste dalla normativa di settore in materia di installazione di impianti audiovisivi e altri strumenti di controllo (art. 4 della l. 300/1970).	Personal computer e documentazione cartacea fax, posta elettronica ordinaria, scanner, stampanti locali e remote, plotter, sistema protocollazione aziendale, Ausilio di software AutoCAD, Primus Software WinWaste Videocamere per sistemi di videosorveglianza fisse e mobili	- NICA Informatica per la sola attività specialistica Flussi rifiuti software WinWaste Innovaway, BOR, Fastweb per servizio di gestione videosorveglianza

Affari Generali (Segreteria e Protocollo)	SECONDO ABILITAZIONI DA SISTEMA: Raccolta, Emissione, Ricevimento di tutte le corrispondenze della Società sia IN/OUT per l'esterno che per le comunicazioni interne. Archiviazione di tutte le comunicazioni della società IN/OUT in qualsiasi forma. Archivio telematico su cloud esterno. Tenuta del registro del protocollo. Invio della corrispondenza aziendale in uscita. SECONDO ABILITAZIONI DA SISTEMA: Gestione corrispondenza entrata ed uscita, archiviazione a sistema di tutte le comunicazioni della società IN/OUT con riferimento anche alle corrispondenze interne.	Personal computer e documentazione cartacea, posta elettronica certificata, sistema protocollazione aziendale, fax, scanner, stampanti locali e remote, collegamenti telematici Utilizzo della Firma digitale dell'Amministratore Personal computer e documentazione cartacea, posta elettronica certificata, sistema protocollazione aziendale, fax, scanner, stampanti locali e remote, collegamenti telematici Firma digitale dell'Amministratore	- DEDA Group per l'attività di gestione del protocollo informatico CIVILIA Next e conservazione sostitutiva dei dati su cloud esterno
Segreteria Tecnica ed Area Tecnica	SECONDO ABILITAZIONI DA SISTEMA: Raccolta, Emissione, Ricevimento della corrispondenza tecnica interna della società, incluso quella contabile, SAL, certificati di buona esecuzione, attestati di buona esecuzione, etc. Archiviazione di tutta la corrispondenza tecnica interna della società, incluso quella contabile, SAL e certificati di buona esecuzione.	Personal computer e documentazione cartacea, sistema protocollazione aziendale, fax, scanner, stampanti locali e remote, collegamenti telematici	- DEDA Group per l'attività di gestione del protocollo informatico CIVILIA Next e conservazione sostitutiva dei dati su cloud esterno
Affari Generali (ITC gestione Rete Dati aziendale)	Gestione diretta, con personale interno di assistenza e manutenzione dell'intera Rete informatica della società e dei domini aziendali direttamente o anche a mezzo postazione remota. Dati in essa contenuti e/o conservati. Manutenzione apparecchiature in dotazione PC, stampanti, etc.	Personal computer e documentazione cartacea, collegamenti telematici, collegamento in remoto su server aziendale, Server di rete, Cloud esterno Telecom	Specialista esterno per il riferimento ITC aziendale e supervisione all'attività effettuata da personale interno

3.4. L'analisi del rischio che incombe sui dati

L'analisi dei rischi, ovvero la valutazione delle possibili minacce in termini di probabilità di occorrenza e relativo danno potenziale, ha l'obiettivo di individuare i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutare le vulnerabilità intrinseche e prevenire le possibili conseguenze o limitarne la gravità, in relazione al contesto fisico-ambientale di riferimento. Nel caso specifico della S.A.P.NA. S.p.A., l'analisi dei rischi che gravano sui dati, viene effettuata combinando due tipi di rilevazioni: a) la tipologia dei dati trattati, nonché la loro pericolosità per la privacy dei soggetti cui essi si riferiscono; b) le caratteristiche degli strumenti utilizzati per il trattamento degli stessi dati. Su tali basi, pertanto, è sviluppata l'analisi dei rischi che prevede la seguente successione di azioni, adottata quale standard procedurale nella valutazione, nonchè in caso di emersione di un nuovo rischio:

1. identificazione dei rischi che possono presentarsi (assessment);
2. impatto consequenziale nel caso di avveramento e priorità di intervento;
3. valutazione e adozione delle contromisure e dei presidi;
4. intervento e tempistiche per la pianificazione delle contromisure.

Periodicamente, e secondo un calendario semestrale, la S.A.P.NA. S.p.A. valuta ed analizza i rischi secondo i passi stabiliti nei precedenti punti, verificando così anche l'eventuale ingresso di nuovi rischi. L'analisi viene condotta previa verifica dell'efficacia delle misure preventive e dei presidi.

A valle dell'analisi la S.A.P.NA. S.p.A. procede con la gestione del rischio specifico, attuando le possibili misure applicabili nell'immediato e pianificando i provvedimenti necessari per mitigare o eliminarne le conseguenze, procedendo, parimenti, al controllo sull'eventuale insorgere di nuovi rischi e verifica sull'attuazione delle contromisure atte alla riduzione/annullamento del livello di rischio.

Con l'eventuale evoluzione della Società e/o delle Norme in materia di salvaguardia dei dati personali potranno effettuarsi adeguamenti e/o miglioramenti strutturali, anche più complessi di quelli già attuati, riguardanti vari aspetti della sicurezza

ad ampio raggio, come ad esempio riguardanti i settori organizzativo, delle risorse umane, della regolamentazione e procedurale, tecnologico, logistico.

3.5. Mantenimento dell'integrità del dato: luoghi presso i quali avviene il trattamento dei dati – UFFICI della SEDE OPERATIVA

I dati di cui al precedente par. 3.1 sono trattati interamente presso la sede operativa della S.A.P.NA. S.p.A. ubicata in Via Ponte dei Francesi, 37/E - 80146 – Napoli.
Nelle altre sedi della Società come, ad esempio, gli impianti STIR di Giugliano e Tufino ed i Siti e le Discariche, non viene trattata la totalità dei dati come avviene per la sede operativa, ed il trattamento/informazioni disponibili sono limitate a:

- informazioni di carattere anagrafico per il personale dipendente;
- informazioni sulle ore lavorate, straordinari, permessi, attività sindacali, etc.
- informazioni di natura commerciale;
- contratti d'appalto per la Fornitura, Servizi e Lavori, inclusi gli allegati progettuali;
- preventivi per Forniture, Servizi e Lavori;
- documenti fiscali, fatture e corrispondenza clientela.

Pertanto, nel caso delle sedi secondarie oltre alla sede operativa, le misure da adottare per la mitigazione del rischio di danno ai dati e quelle relative alla protezione e al trattamento del dato, saranno identiche per tutte le tipologie ma limitate a quelle previste per le categorie suddette.
In ogni caso, qualora dovessero intervenire cambiamenti nella struttura organizzativa o modifiche alla tipologia del dato trattato, quest'ultimo dovrà essere convenientemente protetto dalle misure previste.
I luoghi di lavoro in cui sono allocate le strutture di protezione, sono di seguito descritti con la premessa che le zone comuni esterne di accesso al fabbricato Uffici della Sede Operativa, sono controllate da telecamere brandeggianti a circuito chiuso, i cui monitor sono ubicati presso la portineria di accesso e visionati da personale S.A.P.NA. S.p.A. durante il giorno (dalle 7,00 alle 16,00) e dal pomeriggio fino al mattino successivo da personale di Istituto di Vigilanza con compiti di vigilanza armata e sorveglianza durante le ore notturne in servizio dalle 16,00 alle 8,00 del mattino successivo.

Corpo Uffici

Gli Uffici della Sede Operativa della S.A.P.NA. S.p.A. sono accessibili dall'esterno per il tramite di passo carrabile a fronte strada, munito di cancello metallico motorizzato comandato a distanza per l'ingresso e l'uscita dei mezzi, nonchè di passo pedonale dotato di telecamera di riconoscimento, citofono ed elettroserratura comandabile dalla portineria per l'accesso di persone.
Tra il passo carrabile e l'ingresso principale agli uffici, prospiciente alla viabilità interna, vi è un box completamente equipaggiato, dotato di impianto luce, F.M. e condizionamento, adibito a guardiola intermedia, presso il quale sono installati i comandi per una sbarra di interdizione ai mezzi motorizzati, sia per l'accesso all'autorimessa sottostante il fabbricato che all'area prospiciente la portineria. Il siffatto presidio non è attivo in quanto il cancello motorizzato d'ingresso è tenuto, in condizioni normali, chiuso e l'accesso è consentito tramite annuncio citofonico, direttamente dal locale portineria di accesso agli uffici posto al piano terra.
L'intero corpo uffici è costituito da un piano posto al livello 0°, e da altri tre piani posti al liv. 1°, liv. 2° e liv. 3° questi ultimi raggiungibili per il tramite di ascensore o scale. Gli uffici della S.A.P.NA. S.p.A. sono dislocati su due piani: il piano 2° presso il quale vi sono gli uffici amministrativi e il piano 3° presso il quale vi sono gli uffici tecnici. Il piano 1° è occupato a partire dal Dicembre dell'anno 2022 da altra società pubblicamente partecipata.
A tutti i piani si accede per il tramite della portineria posta al piano 0°, a mezzo scale o ascensore oppure per il tramite di accesso diretto dal garage sottostante il corpo uffici, per il tramite di scale che portano esclusivamente prima al piano 0° e da questo ai successivi piani. Dalla portineria è possibile attraversare un cortile interno al fabbricato, alla fine del quale si trova un secondo ascensore ed una seconda cassa scale che permettono un ulteriore accesso agli uffici, ma solo dall'interno tramite il cortile.
Vi sono telecamere attive che sorvegliano le zone comuni (solo cortile esterno e cortile interno posti al piano 0°) l'ingresso all'autorimessa ed il cancello di ingresso principale (passo carraio) il cui segnale video è riportato su monitor presenti in

portineria presso la quale vi è il personale addetto. La parte delle aree uffici al piano 0° poste a destra rispetto all'ingresso sono occupate da S.A.P.NA. S.p.A., mentre le aree uffici al piano 0° poste a sinistra rispetto all'ingresso non sono occupate e non sono accessibili. Non vi sono telecamere attive interne né alla cassa scale né sul ballatoio scale. Le aree non utilizzate hanno i relativi accessi chiusi, così come sono chiusi gli accessi del secondo ascensore (disabilitato) e quelli prospicienti la cassa scale dopo il cortile interno.

Tutte le porte di piano di accesso agli uffici sono dotate di serratura a chiave yale e permettono la rapida uscita dall'interno verso l'esterno in caso di emergenza per il tramite di maniglione antipanico.

Accesso al Corpo Uffici

E' convenzionalmente stabilito, per motivi di sicurezza, che i varchi di accesso dall'esterno al corpo uffici, sia carrabile che pedonabile, siano permanentemente chiusi, 24 ore su 24. Gli accessi agli uffici sono costantemente presidiati dalla portineria, sorvegliati durante il giorno e durante la notte.

a) *Accesso per il Personale Dipendente:*

Al fine di poter garantire il facile afflusso del personale dipendente agli uffici, nonché il facile esodo dello stesso a fine attività, l'accesso al corpo uffici è così regolato:

Durante i giorni lavorativi, dal Lunedì al Venerdì, i varchi carrabili sono aperti dalle ore 7,00 fino alle ore 10,00 e dalle ore 15,30 fino alle 17,00 nei giorni lavorativi. Nei giorni festivi i varchi sono sempre chiusi. In caso di attività straordinaria o in casi eccezionali di attività svolte in giorni festivi o non lavorativi, l'Amministrazione del Personale, su indicazione dei Responsabili d'Ufficio incluso il Direttore Tecnico, comunicherà preventivamente, ai preposti alla sorveglianza, i nominativi del personale comandato affinchè questi possano accedere ai luoghi delle attività;

b) *Accesso per il personale non dipendente, visitatori, fornitori, etc.:*

L'accesso occasionale agli uffici da parte di visitatori, fornitori o personale di altre società è consentito previa annotazione, su un apposito registro, degli estremi del documento di riconoscimento da parte del personale addetto alla portineria, del visitatore che riceverà apposito "Pass". Il visitatore dovrà dichiarare agli addetti alla portineria il nome dell'ufficio e/o del dipendente presso cui deve recarsi, affinchè il personale della portineria possa trascrivere su apposito registro tutti i dati di riferimento, inclusa l'ora della visita. A termine visita viene ritirato il "Pass", e trascritta l'ora di uscita del visitatore nel registro. L'orario di visita è previsto durante l'orario di lavoro svolto presso gli Uffici della Sede Operativa. Le visite sono solo per appuntamento. E' fatto obbligo al personale di portineria rifiutare l'ingresso a visitatori che, a seguito di verifica, non abbiano ricevuto riscontro dall'interessato;

c) *Accesso per presentazione plichi per gare, concorsi, sportello TARSU, ufficiali giudiziari, messi, forze dell'ordine:*

L'accesso agli uffici alle forze dell'ordine, ad agenti di PG, messi e ufficiali giudiziari è sempre consentito previa sola esibizione della tessera di riconoscimento con annotazione sul registro del visitatore. L'accesso agli uffici per la presentazione di plichi di gara o concorsi o equivalenti è regolato come per il punto b) a meno che non vi siano motivi di particolare urgenza (tempo utile per la presentazione dell'offerta o della domanda di partecipazione). In tal caso i dati saranno rilevati all'uscita.

Per quanto attiene l'esercizio dello sportello TARSU in ordine alle attività di riscossione coattiva che SAPNA SpA esegue quale attività residuale nell'ambito del contratto di concessione della riscossione della tassa sui rifiuti solidi urbani, gli orari al pubblico sono regolati con opportuno avviso posto all'esterno degli uffici. Indicativamente lo sportello TARSU gestito da personale di altra società, è attivo il Martedì e Giovedì con orario dalle 9,00 alle 12,00 e dalle 14,00 alle 16,00.

Locali e stanze nel Corpo Uffici

I locali e le stanze presenti nel Corpo Uffici sono separati per piano e organizzati in tre aree operative: una prima, dislocata al piano 0° comprende portineria, area tecnica, affari generali, sala formazione, gabinetto per visite mediche e locali archivio, una seconda collocata al piano 2°, comprende l'area Amministrazione e la terza, dislocata al piano 3°, comprende l'area Tecnica.

Tutte le stanze costituenti il corpo uffici sono dotate di porta di ingresso con serrature a chiave e sono accessibili da un unico varco ad eccezione della stanza dell'Amministratore Unico che ha nelle proprie disponibilità un doppio ingresso di cui uno è tenuto sempre chiuso. Le aree al piano

0°, Ricevimento, archivi e formazione, sono così suddivise:

- Gli uffici Affari Generali relativamente all'unità operativa ITC;
- Gli uffici per il personale addetto alla TARSU;
- La Portineria;
- Gli Archivi;
- La sala formazione equipaggiata allo scopo;
- Il locale adibito a gabinetto per le visite mediche;
- Servizi igienici, inclusi quelli HP;

2°, Amministrative e societario, sono così suddivise:

- Gli uffici dell'Amministrazione-Contabilità-Fatturazione Attiva/Passiva;
- Gli uffici Gare-Contratti;
- L' ufficio dell'Amministratore Unico;
- L'ufficio Affari Generali Organizzazione e Controllo,

costituito da più locali:

- Affari Generali
- Segreteria e Protocollo
- Legale e Societario

- Gli uffici dell'Amministrazione del Personale;
- Sala Riunioni istituzionale;
- Locale riunioni Sindacali;
- Archivi amministrativi, segreteria e gare e contratti;
- Archivi Amministrazione del Personale.

Le aree al piano 3°, Tecniche, sono così suddivise:

- L'Ufficio della Direzione Tecnica e Operativa;
- L'ufficio della Segreteria Tecnica;
- Gli Uffici supporto: agli impianti, al RUP a Siti e Discariche;
- Gli Uffici per i Siti e per le Discariche;
- Gli Uffici ingegneria ricerca e sviluppo, gestione energia;
- Gli Uffici Contabilità industriale;
- Gli uffici Flussi, Frazione secca, Frazione Umida;
- Gli Uffici Budget e programmazione, servizi Generali;
- Locale Sala riunioni;
- Altre aree e corridoi comuni a tutto il personale in cui sono ubicati armadi di contenimento documenti archiviati, plotter grafici e stampanti in uso comune per il tramite della rete aziendale.

3.6. Mantenimento dell'integrità del dato: luoghi presso i quali avviene il trattamento dei dati – UFFICI IMPIANTI TMB e UFFICI DISCARICHE/SITI

Impianti TMB

Gli impianti di trattamento del rifiuto denominati TMB, in gestione alla SAPNA SpA ed ubicati presso i Comuni di Giugliano (NA) e Tufino (NA), sono costituiti ognuno da un complesso industriale organizzato per capannoni all'interno dei quali avvengono i processi di trattamento meccanico e biologico del rifiuto; gli interi complessi insistono su aree recintate, queste ultime sorvegliate con telecamere a circuito chiuso. Sono altresì allocate in specifici punti strategici dell'impianto, all'aperto, alcune telecamere di sorveglianza poste a tutela del patrimonio come ad esempio depositi, magazzini, particolari impianti di trattamento, etc. Le telecamere sono tutte di tipo fisso e la loro posizione è utilizzata secondo la normativa vigente.

L'accesso in ingresso e l'uscita, i cui orari e giorni di ingresso sono regolati con specifico disposto a cura del Responsabile, per ogni impianto sono dotati di un varco carraio chiudibile per il tramite di cancello; il varco d'ingresso è sorvegliato per il tramite di una apposita guardiola presso la quale è dislocato personale addetto alla rilevazione di tutti quei soggetti come

ad es. operatori economici, visitatori, mezzi in entrata, etc. che abbiano interessi istituzionalmente previsti o contrattualizzati con SAPNA SpA, adottando la regolamentazione prevista dal documento aziendale *Regolamento RE.17.2019 Rev. 01 del Settembre 2021 per gli accessi agli Impianti, Siti e Discariche in gestione alla S.A.P.NA. S.p.A. ed alla Sede Operativa Uffici* che illustra in dettaglio le regole da seguire per gli accessi e per la sorveglianza.
In caso di non avveramento delle condizioni previste dal regolamento o di specifiche disposizioni emesse dal Responsabile d'Impianto, ogni accesso è vietato.
Gli uffici degli impianti, di norma dislocati presso fabbricati separati da quelli in cui avvengono i processi industriali, effettuano tutte le attività amministrative connesse all'esercizio ed al funzionamento dell'impianto.
Inoltre tutti gli impianti TMB sono dotati di "pese" che hanno il compito di rilevare la quantità di rifiuto conferito presso l'impianto e/o anche il rifiuto posto in uscita avviato al recupero. A tale attività di rilevamento è strettamente connessa quella del dato presente nel documento riportante la dichiarazione del rifiuto conferito in ingresso proveniente da Ente esterno (FIR) o anche riportante la dichiarazione del rifiuto che posto in uscita dall'impianto TMB, viene avviato al recupero presso altri impianti esterni autorizzati.
La tipologia, la qualità e le caratteristiche delle apparecchiature, degli strumenti da ufficio e di tutte le strutture di tipo digitale utilizzate per lo svolgimento dei compiti istituzionali presso gli impianti TMB, consentono di applicare a questi ultimi le stesse prerogative e restrizioni per il trattamento e protezione dei dati previste per gli Uffici della Sede Operativa.
Pertanto gli addetti alle operazioni che comportino l'accesso ai dati effettuata presso gli Impianti TMB dovranno seguire le indicazioni ed adottare tutte le misure necessarie in materia di trattamento e protezione del dato, previste dalla presente procedura.

Siti e Discariche

Come per gli impianti anche i Siti e le Discariche in gestione alla SAPNA SpA sono dotati di piccoli fabbricati adibiti ad uso ufficio e di guardianie per le attività di rilevamento ingressi/uscite. Agli stessi vengono applicati, con specifico riguardo alla tipologia del dato trattato da parte dei dipendenti, le indicazioni ed adottare tutte le misure necessarie in materia di trattamento e protezione del dato, previste dalla presente procedura.

3.7. Mantenimento dell'integrità del dato: tipologia delle misure adottate per la protezione del dato

Le strutture preposte al contenimento ed alla protezione dei dati sono rappresentate da due gruppi significativi:

- Strutture fisiche;
- Strutture di tipo digitale.

Le strutture facenti parte di entrambi i gruppi sono allocate in uffici e/o luoghi di conservazione che possono anche non coincidere con quelli presso i quali avviene il trattamento dei dati (ad esempio caso di "server remoti" o "cloud" esterni, contenenti dati di protocollo o altre informazioni aziendali, o dati completi a seguito di misure di "disaster recovery").

Ai fini della presente procedura le strutture vengono così identificate:

- *Strutture Fisiche*

Tali strutture sono convenzionalmente atte al contenimento ed alla conservazione dei dati principalmente su supporti cartacei: Ogni contenitore il cui accesso è impedito da dispositivi di blocco meccanico (serrature, lucchetti, etc.) come ad esempio contenitori a chiave, cassetti con chiavi, mobilio ad ante chiudibili e armadi metallici con serrature, schedari a chiave, casseforti, etc.

- *Strutture di tipo Digitale*

Tali strutture sono convenzionalmente atte al contenimento ed alla conservazione dei dati su supporto esclusivamente informatico e/o magnetici o CD o fisico informatico (chiavi USB, Hard disk, e assimilati) che possono essere o anche non essere gestiti da appositi software, inclusi anche "cloud" esterni e assimilati: il dato è considerato conservato correttamente quando è contenuto/gestito da ogni sistema il cui accesso è impedito da dispositivi di blocco informatico realizzato per il tramite di sistemi di autenticazione (password) come ad esempio, banca dati informatica, hard disk di PC aziendale, dominio aziendale, server aziendale, cloud esterno per la conservazione di files, hard disk virtuali, etc.

La S.A.P.NA. S.p.A., nell'ambito delle proprie attività, predispone apposite protezioni dei dati ricorrendo alle strutture sopracitate utilizzandole in forma singola, separata o associata.

Tali protezioni sono effettuate, in via generale, anche con la realizzazione di zone controllate per il tramite di sorveglianza, oppure con locali il cui accesso è consentito solo ai possessori di autorizzazioni specifiche e/o delle chiavi di accesso. In questi locali sono ubicate le protezioni fisiche del dato, come ad esempio schedari, armadi metallici chiusi a chiave, casseforti, etc.

Nel caso in cui i dati dovessero essere acquisibili e/o trattati in locali aperti (open space) o uffici sprovvisti dei controlli di sorveglianza, ovvero, in zone in cui l'accesso non viene protetto, il dato sarà disponibile/acquisibile, per il trattamento, solo previo accesso da dispositivi di blocco meccanico (armadi di contenimento di faldoni con ante chiudibili a chiave in possesso di personale autorizzato) o con dispositivi di blocco informatico, in quanto acquisibili solo da sistema.

Tutti gli altri dati, classificati come non soggetti all'obbligo di riservatezza, presenti negli uffici ed in tutte le altre zone aperte, saranno comunque ordinati in raccoglitori chiusi ed allocati in appositi scaffali e/o armadi.

I provvedimenti di base atti alla mitigazione e/o prevenzione del rischio di perdita del dato adottati da S.A.P.NA. S.p.A. consistono nelle seguenti azioni:

- **a)** solo i dati personali vengono sistematicamente tratti con supporti cartacei e con elaborazione;
- **b)** i dati sensibili trattati con elaborazione sono limitati a quelli necessari per assolvere agli obblighi istituzionali, normativi e contrattuali;
- **c)** gli economico/patrimoniali trattati sono quelli strettamente necessari per assolvere gli obblighi normativi e di legge;
- **d)** gli elaboratori sono collegati alla rete aziendale, dispongono esclusivamente del collegamento al dominio aziendale e, per il tramite di esso, al collegamento con gli accessi internet. L'accesso al dominio da parte di ogni singolo computer è soggetto a restrizioni ed è effettuabile solo per il tramite di opportuna password personale in custodia all'utente.
- **e)** Per l'accesso ad ogni singolo elaboratore presso la postazione di lavoro è necessaria una password -personale- per l'accesso al dominio, senza la quale l'elaboratore non potrà accedere alla configurazione ed ai dati custoditi in rete.
- **f)** Per l'accesso in remoto al proprio PC nel caso in cui il lavoratore debba espletare attività in telelavoro o smart-working l'accesso è garantito per il tramite di un'apposita VPN in grado di collegare il PC dell'ufficio con altro in remoto. La modalità di accesso è salvaguardata da Id e Password personali senza le quali non potrà essere possibile l'accesso. Le VPN sono protette dal sistema aziendale antivirus e le policy di protezione applicate al PC aziendale sono le stesse per l'utilizzo in remoto.

3.8. Mantenimento dell'integrità del dato: individuazione del rischio, classificazione e prevenzione

All'interno dei locali degli uffici non sono utilizzati né previsti impianti di video sorveglianza oltre a quello già in precedenza descritto per il solo controllo dell'accesso dall'esterno.

Relativamente al corpo Uffici, sono pertanto classificabili come soggetti a rischio i seguenti strumenti, utilizzati per il trattamento, ed i collegati fattori:

A. Strumento:

Casseforti, schedari, armadi, armadi blindati, contenitori ed altri supporti posti in area non controllata e alla portata di tutto il personale (ad esempio: **Corridoi**).

Rischio:

Rischio d'area legato all'accesso non autorizzato ai locali, agli schedari, agli armadi ed alla documentazione cartacea in essi contenuta;

Provvedimento di protezione:

Struttura Fisica-Segregazione meccanica a mezzo di chiave e serratura consegnata a persona autorizzata. Serrature a Combinazione e/o a chiave speciale consegnata a persona autorizzata.

B. Strumento:

Casseforti, schedari, armadi, contenitori e scaffalature a giorno ed altri supporti posti in area non controllata, protetta con porta di accesso chiudibile con serratura a chiave (ad esempio: (**Archivi**).

Rischio:

Rischio d'area legato all'accesso non autorizzato nei locali;

Provvedimento di protezione:

Struttura Fisica- Segregazione meccanica a mezzo di chiave e serratura, divieto di accesso alle persone non autorizzate, stato "sempre chiuso" della porta di accesso, accesso consentito esclusivamente a persona/e autorizzata/e;

C. Strumento:

Schedari, armadi, contenitori ed altri supporti posti in tutte le aree poste all'interno di uffici, protetti con porta di accesso chiudibile con serratura a chiave.

Rischio:

Rischio d'area legato all'accesso da parte di personale non autorizzato; Rischio d'area per possibili eventi distruttivi nei locali;

Provvedimento di protezione:

Struttura Fisica- Presidio con dispositivi fissi contro l'incendio, Protezione con l'ausilio di mezzi meccanici contro la penetrazione e l'accesso di soggetti non autorizzati; Cartelli monitori, provvedimenti meccanici di chiusura degli armadi, delle cassettiere, degli schedari (ad esempio: **uffici e postazioni di lavoro**)

D. Strumento:

Computers da tavolo e portatili, server, hard disk esterni, sistema rete aziendale su supporto informatico interno o esterno, software gestionali e/o software di supporto all'attività della Società, switch di rete ed altre apparecchiature, server, posti in appositi locali tecnici

Rischio:

Rischio d'area legato all' accesso non autorizzato a dati su strumenti informatici, Manomissione dello strumento informatico, perdita dei dati, introduzione di virus nel sistema di rete aziendale, rischio d'area per possibili eventi distruttivi nei locali;

Provvedimento di protezione:

Struttura Fisica e Struttura Digitale, la protezione è realizzata con l'ausilio di mezzi meccanici contro la l'accesso di soggetti non autorizzati ai server aziendali; la protezione di accesso all'uso dell'elaboratore è realizzata con l'ausilio di blocco informatico realizzato per il tramite di sistemi di autenticazione (password) sia per i PC aziendali che per i server; Protezione con sistemi antivirus della rete interna e con firewall per la connessione all'esterno; chiusura meccanica con serratura delle porte di accesso ai locali tecnici.

Periodicamente, con cadenza trimestrale, verranno attuate misure preventive di verifica e controllo generale sullo stato di sicurezza, alle modalità del trattamento di dati personali e agli strumenti utilizzati, verificando l'efficacia delle misure adottate relativamente a:

- accesso fisico ai locali dove si svolge il trattamento;
- procedure di archiviazione e custodia dei dati trattati;
- efficacia e utilizzo delle misure di sicurezza degli strumenti elettronici;
- integrità dei dati e delle loro copie di backup;
- distruzione dei supporti magnetici non più riutilizzabili;
- livello di informazione degli interessati;
- richiesta automatica di cambio periodico delle password di accesso;

3.9. Criteri e modalità di ripristino in seguito a perdita del dato

E' necessario identificare innanzitutto le cause che possono portare alla perdita del dato, che nel caso della S.A.P.NA. S.p.A. possono essere ricondotte ai seguenti eventi:

- Perdita del dato a seguito di eventi accidentali
- Perdita del dato a seguito di errore umano
- Perdita del dato a seguito di attacchi volontari al dato stesso

Per i dati trattati con strumenti elettronici sono previste procedure di backup attraverso le quali viene periodicamente effettuata una copia di tutti i dati presenti nel sistema, il salvataggio dati avviene con frequenza quotidiana e le copie dei dati vengono custodite su server dedicato. I dati processati attraverso apposito software di gestione, come fatturazione elettronica, protocolli ed assimilati vengono altresì custoditi in conservatoria in apposito cloud esterno.

I dati cartacei sono custoditi in appositi archivi presso locali adibiti esclusivamente a tale scopo. La protezione da eventuale perdita del dato, nel caso in cui questo sia conservato solo sotto forma di documento cartaceo, è assicurata oltre che da misure meccaniche – come ad esempio serrature a chiave, cassetti a chiave, etc. - anche da misure di sicurezza quali antincendio, mantenimento di temperatura e ricambi d'aria costanti.

3.10. Programma della Formazione

La formazione in materia di trattamento dei dati personali/sensibili e sulla riservatezza degli stessi viene effettuata, compatibilmente con le necessità aziendali, in modo periodico e sistematico su tutto il personale interessato, articolandola su tre livelli di cui al precedente par. 2.3. del presente documento, ovvero:

- **Livello I° A.** Il Titolare del trattamento dati di S.A.P.NA. S.p.A.;
- **Livello II° B.** Il Responsabile del trattamento dati preposto dal Titolare;
- **Livello III° C.** Gli Addetti che abitualmente/occasionalmente trattano dati di S.A.P.NA. S.p.A.;

La formazione interesserà sia le norme generali in materia di privacy sia gli aspetti peculiari dei trattamenti effettuati.

- La formazione di I° Livello è effettuata "ad hoc" per il solo Titolare del trattamento dei dati di S.A.P.NA. S.p.A., il quale dovrà partecipare anche alla formazione nelle tipologie di II° e III° livello. Nel caso in cui il titolare del trattamento dovesse cambiare, la S.A.P.NA. S.p.A. provvederà ad effettuare la stessa formazione per il nuovo soggetto subentrante.

  Il programma di formazione specifica dovrà essere calibrato in funzione della responsabilità della titolarità e del ruolo ricoperto in azienda.

  Per tutti i livelli di formazione, l'istruzione dovrà comprendere, quali elementi di base, la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza, in caso di trattamenti di dati personali affidati, in conformità al codice, alla S.A.P.NA. S.p.A. nonché all'esterno della struttura del titolare. Inoltre specifica istruzione dovrà essere adottata, nel programma di formazione, per il trattamento di quei dati personali idonei a rivelare lo stato di salute e la vita sessuale e l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.
- La formazione di II° Livello è effettuata per tutti coloro che sono stati preposti al trattamento dati, in una specifica funzione o area aziendale, con specifica nomina da parte del Titolare. Anche in questo caso il programma di formazione specifica dovrà essere calibrato in funzione della responsabilità della titolarità e del ruolo ricoperto in azienda.
- La formazione di III° Livello, infine, è effettuata per tutto il personale dipendente di S.A.P.NA. S.p.A. che abitualmente/occasionalmente trattano o siano in contatto totale o parziale con i dati detenuti da S.A.P.NA. S.p.A. Il relativo programma di formazione specifica riguarderà i requisiti minimi da rispettare e le precauzioni necessarie affinchè vengano rispettate le norme in materia di trattamento dati personali e/o sensibili.

Sono previsti corsi di aggiornamento nell'ipotesi d'introduzione di nuovi strumenti e/o programmi informatici e, comunque, per il personale neoassunto o con nuova mansione.

4. Affidamento dei dati personali a terzi

Nel caso in cui lo svolgimento di attività aziendali che includono il trattamento di dati personali e/o di dati sensibili, fossero affidate in outsourcing a strutture esterne alla S.A.P.NA. S.p.A., ciascuna struttura dovrà trasmettere al Titolare del Trattamento di S.A.P.NA. S.p.A., il proprio documento in ordine alle misure di protezione adottate, il nominativo del proprio Titolare e i riferimenti/indirizzi per le comunicazioni con quest'ultimo. In mancanza, il titolare della struttura esterna dovrà firmare un documento, redatto su propria carta intestata, con il quale si dichiara di aver letto, compreso e di rispettare la

presente procedura in materia di trattamento dei dati, nonchè di rispettare quanto prescritto dal codice della privacy per tutta la durata del rapporto intrattenuto con la S.A.P.NA. S.p.A. **In alternativa o in mancanza, il documento sarà approntato da SAPNA SpA e posto alla firma dell'operatore esterno, senza la quale non potrà procedere al trattamento del dato.**

5. Modalità di Trasmissione documenti

La trasmissione dei documenti avviene per il tramite di sistema protocollare e/o telematico, incluse le comunicazioni interne tra dipendenti. Qualora, per esclusivi motivi di riservatezza o in occasione di guasti tecnici prolungati, non venisse utilizzata una trasmissione di tipo telematico o protocollare che permetta la tracciabilità e la protezione da lettura indebita del documento trasmesso, i documenti cartacei possono essere trasmessi all'interno della S.A.P.NA. S.p.A. in forma protetta ai rispettivi destinatari e a ciascuno per le rispettive competenze e con le rispettive finalità. Anche in questo caso i destinatari di tali documentazioni dovranno attenersi agli obblighi di riservatezza ed alle misure di protezione del dato previste dalla presente procedura. Nei confronti di terzi (consulenti esterni, strutture esterne che prestano la propria attività in outsourcing, etc.) l'eventuale trasmissione dei dati avviene in forma telematica previa firma di documento di riservatezza. Agli stessi viene applicata la regola di cui al precedente p.4.

6. Modalità di trattamento del Dato

Sono previsti:

a) Trattamento dei dati personali dei dipendenti e dei collaboratori professionali, necessari alla corretta gestione del rapporto di lavoro, connessi alla reperibilità e alla corrispondenza con gli stessi o richiesti ai fini fiscali e previdenziali, o dati di natura bancaria. L'elaborazione delle paghe e la stampa dei relativi cedolini avviene all'interno degli uffici della sede operativa e le relative attività vengono svolte dal personale preposto, autorizzato, che utilizza specifici software il cui accesso è protetto da password. Al trattamento di tali dati concorre, per la sola parte degli adempimenti fiscali, una struttura esterna, nella specie uno studio professionale specializzato in materia tributaria e fiscale del lavoro, dotato delle necessarie abilitazioni, al quale è richiesto di rilasciare una dichiarazione di conformità alle misure minime di sicurezza della sua struttura. Il trattamento dei dati personali dei dipendenti può comportare anche il trattamento dei dati sensibili dei dipendenti stessi;

b) Trattamento dei dati finanziari della Società, necessari alla corretta gestione delle finanze e delle contabilità aziendali, provenienti da conti correnti bancari e dall'operatività per il pagamento di imposte, tasse, contributi, oneri assicurativi, etc.;

c) Trattamento dei dati personali di fornitori e terzi provenienti da albi, elenchi pubblici, visure camerali oppure concernenti la corrispondenza con gli stessi, nonché i dati necessari ai fini fiscali o i dati di natura bancaria per le operazioni di pagamento;

6.1. Misure di sicurezza generali

Per misure di sicurezza deve intendersi l'insieme delle prescrizioni di carattere tecnologico, procedurale ed organizzativo finalizzate all'implementazione di un adeguato livello di sicurezza nel trattamento dei dati.

I dati e le informazioni di carattere sensibile e/o giudiziario devono essere trattati in aree protette, anche fisicamente, dall'accesso di persone non autorizzate. Sono perciò individuati spazi, presso ciascun ufficio per il trattamento e la conservazione dei dati sensibili e giudiziari. Il personale in servizio presso l'Azienda ha eventualmente accesso alla consultazione di tali dati esclusivamente per l'adempimento della prestazione lavorativa.

Il personale che espleta servizi strumentali (es.: pulizia dei locali) o si occupa della manutenzione e dei servizi accessori, deve essere espressamente autorizzato ad accedere alle aree di sicurezza.

Negli spazi di lavoro va impedita la promiscuità di permanenza tra:

- personale incaricato del trattamento di dati personali;
- personale non incaricato di trattamento di dati personali;
- soggetti estranei all'azienda.

Il personale dipendente ha accesso ai dati esclusivamente sulla base delle esigenze di servizio, conformemente ai seguenti principi:

- la necessità di trattamento;
- l'utilità, per lo svolgimento dell'attività lavorativa, di un livello minimo di conoscenza dei dati.

Il Responsabile del trattamento deve vigilare affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche di dati o ove vengono trattati dati sensibili o giudiziari. E' altresì compito del Responsabile vigilare sull'introduzione in tali aree di oggetti, apparecchiature, sostanze o materiali che possono favorire il sorgere di rischi.

Devono essere previsti procedure, accorgimenti e strumenti per:

- consentire l'accesso alle aree dove vengono custoditi e trattati i dati al solo personale autorizzato;
- ostacolare l'accesso abusivo ai dati;
- segnalare la presenza di intrusi.

6.2. Archivi cartacei

Ferma restando la necessità prioritaria di tenere archivi di tipo digitale, in osservanza alle norme sulla digitalizzazione dei documenti, gestiti utilizzando sistemi protocollari di archiviazione e conservazione certificati, la gestione degli archivi cartacei dei documenti contenenti i dati sensibili e/o giudiziari ed altra documentazione attinente dovrà essere custodita in armadi dotati di serratura, le cui chiavi dovranno essere conservate in modo appropriato.

I documenti contenenti dati sensibili o giudiziari devono essere conservati secondo modalità che precludano la visione, in occasione della consultazione di documenti di altro genere, anche mediante creazione di fascicoli in busta chiusa, con sottoscrizione del Responsabile incaricato del trattamento di quei dati. Il Responsabile, infatti, deve garantire l'integrità dei fascicoli in occasione dell'accesso all'archivio da parte di soggetti non legittimati alla consultazione dei dati sensibili o giudiziari.

7. Istruzioni per il Trattamento dei Dati

Le seguenti istruzioni costituiscono una serie organica di prescrizioni, orientate a garantire la sicurezza dei dati e delle informazioni detenute dagli uffici e dalle strutture della SAP.NA. S.p.A.

Tali prescrizioni devono intendersi come istruzioni impartite, ai sensi dell'art. 29, comma 5 del decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali. Lo scopo delle prescrizioni è quello di evitare il rischio di danneggiamento o dispersione dei dati, in conformità di un trattamento corretto.

In ogni caso, il trattamento dei dati presso gli uffici e le strutture dell'Azienda deve avvenire:

- nel rispetto del principio di riservatezza;
- in modo lecito e secondo correttezza;
- per un periodo di tempo non superiore a quello necessario agli scopi per i quali i dati sono stati raccolti e, successivamente, trattati;
- nel rispetto delle misure minime di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Nello specifico, deve intendersi per:

- **Tutela della riservatezza**: l'attivazione di procedure di conoscenza delle informazioni detenute, a qualsiasi titolo, dall'Azienda, tali da consentire l'accesso solo a soggetti identificati e dotati di un adeguato grado di autorizzazione;
- **Integrità:** l'aggiornamento dei dati e delle informazioni realizzato periodicamente da personale autorizzato;
- **Disponibilità:** l'attivazione di procedure che consentano ai soggetti autorizzati di accedere in tempi utili alle informazioni.

Le istruzioni di seguito riportate intendono quindi individuare modalità operative che rafforzino la sicurezza del trattamento dei dati.

7.1. Istruzioni per il trattamento e protezione dei dati: "documenti in ingresso"

Per "documenti in ingresso", si intendono i documenti o i supporti contenenti dati personali acquisiti dalla società ai fini di un loro impiego in trattamento.

Relativamente al trattamento dei documenti in ingresso, è necessario adottare le cautele seguenti:

a) i documenti in ingresso devono essere utilizzati soltanto da chi sia Incaricato al trattamento dei dati che contengono o dal Responsabile;

b) l'Incaricato deve verificare:

- la provenienza dei documenti;
- la tipologia dei dati contenuti (identificativi, personali, sensibili, giudiziari, …), al fine di individuare le modalità legittime ed idonee per il trattamento e le misure di sicurezza da attuare;
- l'osservanza del principio di pertinenza e non eccedenza rispetto o alle finalità del trattamento, la completezza, la correttezza e l'aggiornamento dei dati.

A tale scopo è utilizzato il programma software "Folium" che consente, per il tramite delle opportune abilitazioni, utilizzando apposite password ed Id di accesso, di dare gli stessi solo all'ufficio che ne è il corretto destinatario e provvedere nel contempo all'archiviazione ed alla conservazione.

Inoltre, la distribuzione dei documenti contenenti dati sensibili viene impedita "mediante l'istituzione di protocolli classificati" con livelli di riservatezza man mano crescenti consentendo l'accesso ad essi solo agli uffici competenti al relativo trattamento.

Il Responsabile del trattamento dei dati è tenuto ad effettuare controlli sulle attività degli incaricati del trattamento, al fine di garantire la puntuale applicazione delle disposizioni contenute nel Codice. Il responsabile, preferibilmente, precisa le istruzioni per il corretto trattamento dei dati, in forma scritta. E' sempre ammessa la diffusione di istruzioni in forma orale, in particolare allorquando vi sia l'urgenza di salvaguardare i principi in materia di trattamento dei dati personali.

7.2. Custodia

I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili alle persone non incaricate del trattamento, mediante localizzazione presso spazi con accesso riservato (es. armadi o cassetti chiusi a chiave). I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, devono essere ivi collocati al termine della giornata e non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

7.3. Comunicazione

La diffusione dei dati personali deve avvenire in base al principio dello "minimo indispensabile", talché non devono essere condivisi, comunicati o inviati a soggetti che non ne abbiano bisogno per lo svolgimento delle funzioni lavorative, a prescindere dall'eventuale qualifica di responsabili o incaricati di altra struttura. I dati non devono essere comunicati all'esterno della struttura, e comunque a soggetti terzi, se non previa autorizzazione.

7.4. Distruzione

Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere soppressi mediante apparecchi "distruggi documenti" o, in assenza, attraverso modalità che impediscano qualsiasi ricomposizione. I supporti magnetici contenenti dati personali o sensibili devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti secondo modalità che ne impediscano la ricomposizione.

7.5. Istruzioni per il trattamento di dati sensibili e/o giudiziari

I documenti contenenti dati sensibili e/o giudiziari devono essere sottoposti al controllo dei Responsabili i quali, a loro volta, potranno avvalersi degli incaricati per la custodia e/o il trattamento. Il Responsabile deve impedire l'accesso a persone prive di autorizzazione nei luoghi e nei momenti in cui si trattano dati sensibili e/o giudiziari; conseguentemente, il trattamento di dati sensibili e/o giudiziari contenuti in documenti cartacei deve avvenire per il tempo strettamente necessario al trattamento, con successiva immediata archiviazione dei dati in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

Per accedere agli archivi, anche informatici, contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario essere in possesso di un'autorizzazione scritta da parte del proprio Responsabile che la rilascerà sentito il Titolare del Trattamento.

7.6. Trattamenti senza l'ausilio di strumenti elettronici

Il trattamento di dati senza strumenti elettronici coinvolge i dati contenuti in tutti i supporti cartacei o simili che, comunque non richiedano l'uso di elaboratori elettronici. Ove esistano copie o riproduzioni di documenti che contengono dati personali, le medesime devono essere protette con le stesse misure di sicurezza applicate agli originali.

7.7. Trattamenti con l'ausilio di mezzi elettronici

Per trattare i dati mediante dispositivi informatici, deve seguirsi una procedura di autenticazione che consenta l'identificazione dell'utente, mediante "credenziali di autenticazione". Le "credenziali di autenticazione" consistono in un user-ID, associato ad una parola chiave segreta denominata password. Le user-ID e password individuali per l'accesso alle applicazioni non possono essere condivise con altri soggetti, anche se incaricati del trattamento. Per i PC collegati in rete, gli utenti devono superare le procedure di identificazione, quali formalità preliminari per accedere alle risorse presenti nella rete aziendale; nel caso di utilizzo di applicazioni centralizzate, gli utenti devono provvedere anche alla propria identificazione sul sistema applicativo centrale, secondo le modalità e le regole previste dall'applicativo stesso.
Tutti coloro che utilizzano un personal computer per il trattamento di dati personali non collegato in rete, sono tenuti a proteggere l'accesso alla propria postazione di lavoro attivando una password.

7.8. Gestione delle password

I Responsabili devono garantire l'esclusività dell'uso della password, in particolare impedendo che incaricati, o altri, si avvalgano di credenziali di autenticazione a qualunque titolo percepite.

7.9. Presenza di estranei all'azienda

I Responsabili devono garantire che le attività degli incaricati non vengano espletate alla presenza o secondo modalità che consentano ad estranei, di acquisire dati e/o informazioni detenute dall'azienda. A tal fine i Responsabili devono impartire istruzioni finalizzate ad evitare che personale estraneo o visitatori restino negli spazi ove si trattano dati personali. In ogni caso,
gli incaricati sono tenuti a riporre i documenti contenenti dati personali secondo modalità che ne impediscano la visione a qualunque soggetto non legittimato.

7.10. Istruzioni per il trattamento di dati sensibili sanitari

I dati anagrafici devono essere conservati separatamente da quelli sanitari che, invece, vanno conservati in apposita "cartella sanitaria" consultabile ed aggiornabile solo ed esclusivamente dal medico competente incaricato dalla Società. Tali dati dovranno essere custoditi in forma segregata e separata da tutti gli altri.

8. Introduzione all'organizzazione informatica di S.A.P.NA. S.p.A.

8.1. Struttura Fisica

Il nodo principale di arrivo Telecom è ubicato nel rack gestore dati e telefonico del locale tecnico al 3° Piano, nel quale sono allocati n. 2 server, i patch panels, gli switch di distribuzione rete orizzontale dei locali del 3° Piano agli utenti, i collegamenti telefonici e i collegamenti in verticale con i locali tecnici del 2° Piano. Al punto di arrivo Telecom è predisposto anche un pannello FO per la connessione in fibra ottica di fornitura Telecom. Parimenti è connesso in verticale con cavo in fibra ottica il 3° Piano con il 2° Piano per il tramite di appositi pannelli di interconnessione tra i rispettivi rack. Al 2° Piano, nel dedicato Locale Tecnico, è allocato un altro rack nel quale sono installati gli switch di distribuzione orizzontale rete dei locali del 2° Piano agli utenti, i collegamenti telefonici e i collegamenti in verticale provenienti dai locali tecnici del 3° Piano. La distribuzione di rete dati avviene a partire dagli switch singolarmente, a mezzo cavo in rame 4cp cat.6, direttamente dalla porta di uscita fino alla presa RJ45 dell'utente, senza interposizione di apparecchi o dispositivi intermedi. Le patch cord utilizzate per le connessioni dalla presa al PC e per le connessioni agli switch sono di tipo preformato.
Le informazioni e le descrizioni relative all'infrastruttura Server che si è consolidata in ambiente *CLOUD TIM* e tutti i sistemi messi in opera per la difesa perimetrale e la sicurezza dei dati aziendali da eventuali attacchi informatici, sono rappresentate di seguito. Verranno pertanto descritte le infrastrutture che compongono l'area CLOUD e Security aziendale, i metodi di accesso e le architetture che le contraddistinguono.

8.2. Descrizione dell'Infrastruttura CLOUD

Dal 2019 si è iniziato il processo di consolidamento dei server aziendali in ambiente virtuale, al fine di garantire maggiore flessibilità e sicurezza per l'erogazione dei servizi.
Vista la possibilità di accedere ai sistemi messi a disposizione da CONSIP, si è deciso di aderire alla convenzione SPC CLOUD LOTTO 1 per la sottoscrizione di un ambiente CLOUD di tipo IaaS (Infrastructure as a Service).
Tale scelta ha fornito le basi per migrare e consolidare i servizi aziendali che sono così confluiti nell'ambiente a noi dedicato.
L'ambiente IaaS è gestito tramite hypervisor HPE Helion OpenStack ed è direttamente connesso tramite collegamento interno alla rete MPLS aziendale della S.A.P.NA.
Il portale per la configurazione dell'infrastruttura è accessibile alla seguente URL previa autenticazione:

- https://cs4.cloudspc.it/auth/login/?next=/

L'utilizzo e configurazione dell'ambiente "as is" è il seguente:

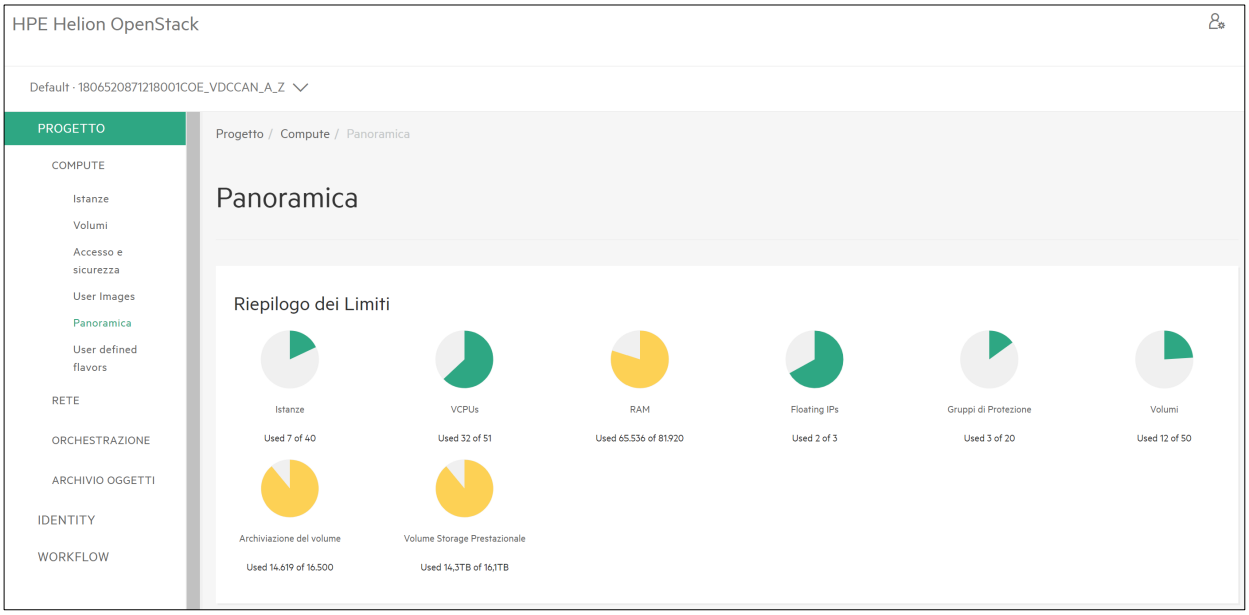


Figura 1

Le risorse impegnate alla data del presente documento sono di seguito riassunte:

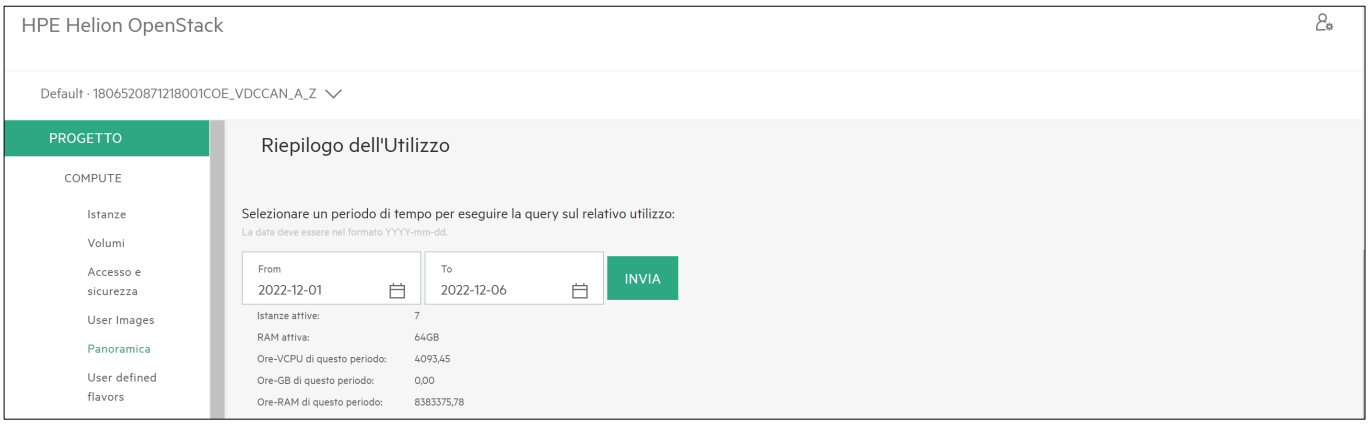


Figura 2

I server attualmente configurati alla data del documento sono:

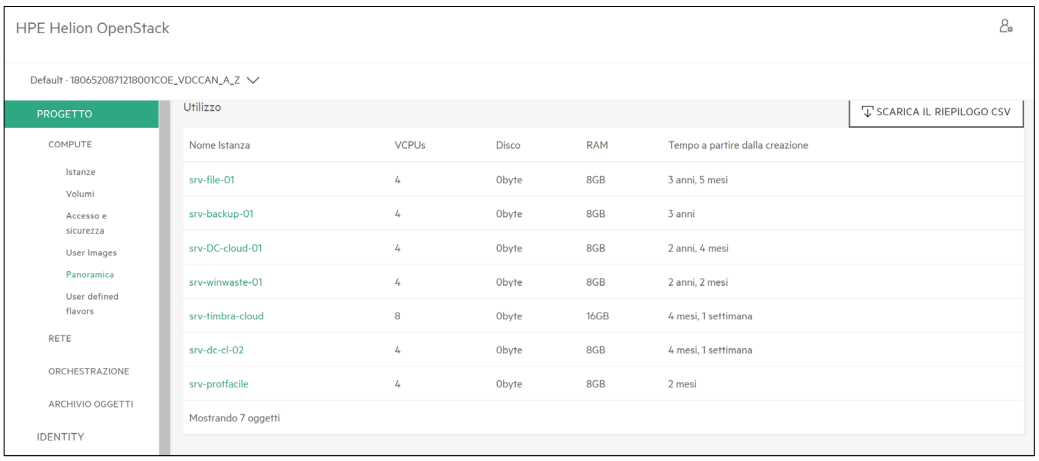


Figura 3

I cui Volumi associati alla VM sono:

Nome	Dimensione	Stato	Tipo	Collegato a	Avviabile
HD-ProtFacile-01	1000GiB	In uso	Prestazionale	Collegato a srv-protfacile su /dev/vda	Sì
HD-timbra01-cl-disk1	500GiB	In uso	Prestazionale	Collegato a srv-timbra-cloud su /dev/vda	Sì
HD-dc02-cl-disk1	160GiB	In uso	Prestazionale	Collegato a srv-dc-cl-02 su /dev/vda	Sì
HD_Backup_02	3000GiB	In uso	Prestazionale	Collegato a srv-backup-01 su /dev/vdc	No
HD DATI FILE SERVER 02	2000GiB	In uso	Prestazionale	Collegato a srv-winwaste-01 su /dev/vdb	No
W2K12_r2_File_02	160GiB	In uso	Prestazionale	Collegato a srv-winwaste-01 su /dev/vda	Sì
W2K12_r2_DC_cloud_01	160GiB	In uso	Prestazionale	Collegato a srv-DC-cloud-01 su /dev/vda	Sì
HD BACKUP 1	4999GiB	In uso	Prestazionale	Collegato a srv-backup-01 su /dev/vdb	No
HD DATI FILE SERVER	2000GiB	In uso	Prestazionale	Collegato a srv-file-01 su /dev/vdb	No
518cdd13-b08b-4d29-ac0a-b6fc9703a70a	160GiB	In uso	Prestazionale	Collegato a srv-backup-01 su /dev/vda	Sì
W2K12_r2_App_01	160GiB	Disponibile	Prestazionale		Sì
W2K12_r2_File_01	160GiB	In uso	Prestazionale	Collegato a srv-file-01 su /dev/vda	Sì

Tabella 2

Ad oggi, i 7 server virtuali ospitati nell'ambiente cloud compongono l'intero panorama dei sistemi SAPNA SpA, con eccezione di un unico server fisico che ha il compito di assicurare la necessaria ridondanza al fine della conservazione in copia sincronizzata dei dati aziendali.

L'infrastruttura generale è quindi così schematizzata:

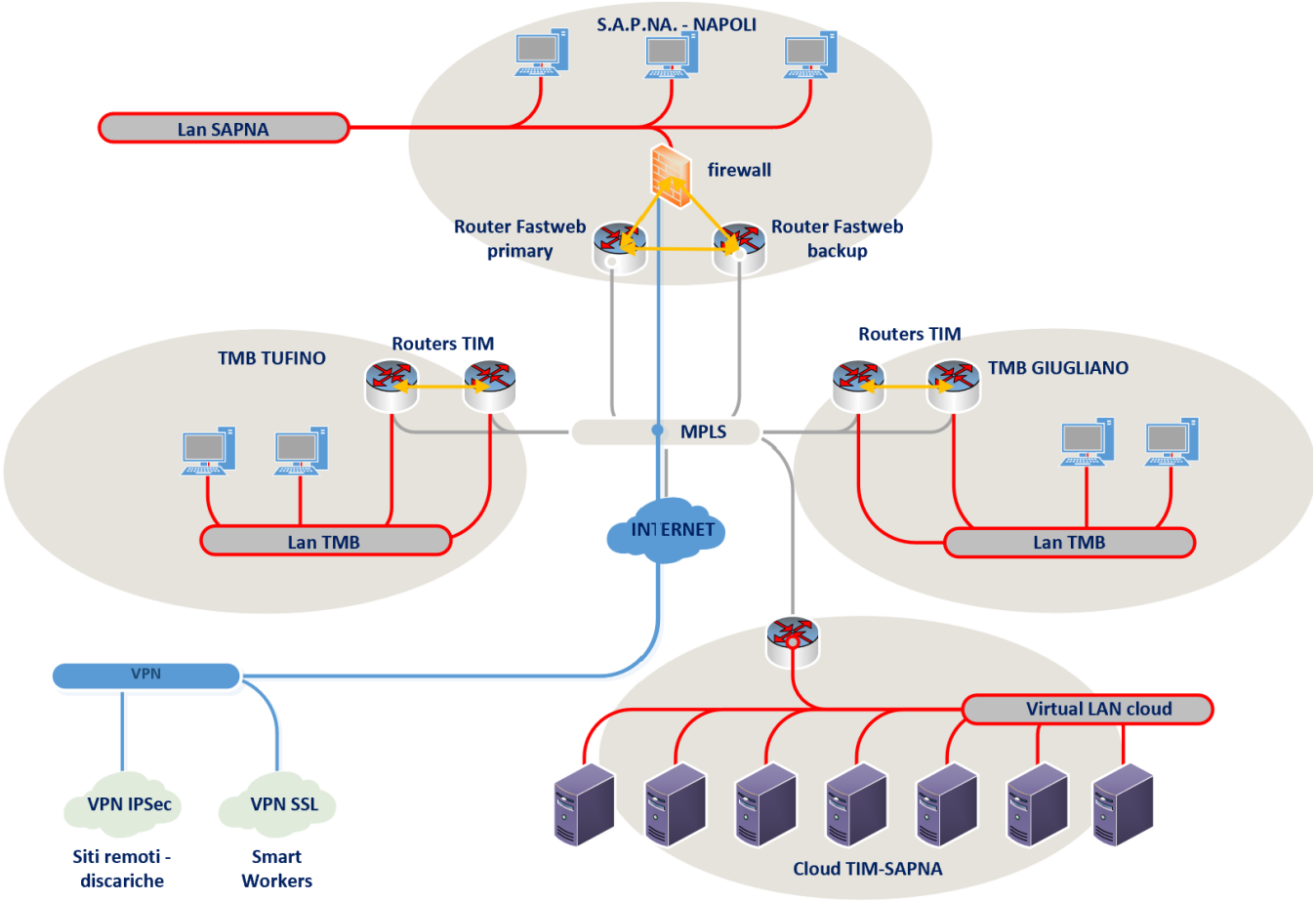


Figura 4

8.3. Descrizione dei singoli server in Cloud

Il CLOUD TIM ospita all'interno del Data Center di Rozzano (MI) l'infrastruttura IaaS dedicata a S.A.P.NA., all'interno della quale sono stati configurati i seguenti server con i relativi servizi:

nome VM	caratteristiche			IP	Sistema Operativo
	vCPUs	RAM	Disco		
Srv-DC-cloud-01	4	8	160GB	192.168.9.15/24	Windows Server 2019 DataCenter
Srv-DC-cloud-02	4	8	160GB	192.168.9.25/24	Windows Server 2019 DataCenter
Srv-file-01	4	8	2,16TB	192.168.9.9/24	Windows Server 2012 DataCenter
Srv-backup-01	4	8	8TB	192.168.9.10/24	Windows Server 2012 DataCenter
Srv-winwaste-01	4	8	2,16TB	192.168.9.19/24	Windows Server 2012 DataCenter
Srv-Timbra-cloud	8	16	500GB	192.168.9.24/24	Windows Server 2019 DataCenter
Srv-ProtFacile	4	8	1TB	192.168.9.27/24	Windows Server 2019 DataCenter

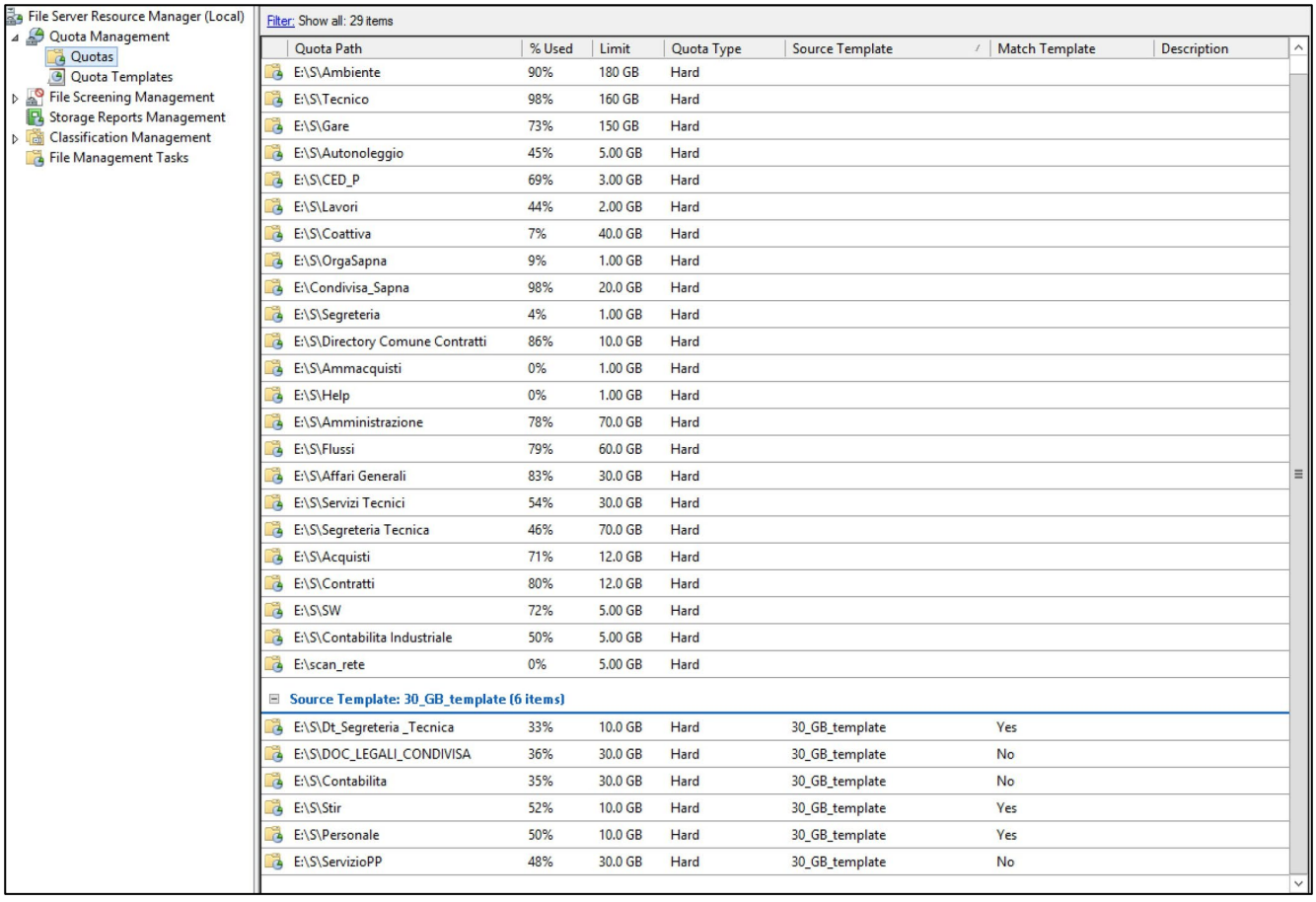
Tabella 3

8.3.1. Elenco servizi erogati

- I Server DC-cloud-01 e 02 hanno funzione di Domain Controller, necessari durante il processo di autenticazione ai computer aziendali e sono stati recentemente aggiornati, ad oggi i server offrono i seguenti servizi:

- Active Directory, functional level 2016 sia per il dominio che per la forest
- DNS, per le zone:
  - sapnapoli.local
  - 9.168.192
  - 10.168.192
  - 31.168.192
  - 32.168.192
- Distribuited File System (DFS), per l'accesso alle risorse condivise di rete

➢ Il Server FILE-01 ha il ruolo di file server, è un server di dominio e fornisce l'accesso alle cartelle di rete condivise da lui ospitate sulle quali è abilitato anche l'auditing per il tracciamento delle azioni sui file.
Il ruolo è gestito tramite servizio DFSR, per il quale è anche abilitata la funzione di Access Based Enumeration (ABE) per la visualizzazione selettiva delle cartelle in funzione degli effettivi permessi NTFS associati.
L'elenco delle cartelle gestite dal FILE SERVER ed il relativo stato della Quota di occupazione del disco è di seguito riportato:



Quota Path	% Used	Limit	Quota Type	Source Template	Match Template	Description
E:\S\Ambiente	90%	180 GB	Hard			
E:\S\Tecnico	98%	160 GB	Hard			
E:\S\Gare	73%	150 GB	Hard			
E:\S\Autonoleggio	45%	5.00 GB	Hard			
E:\S\CED_P	69%	3.00 GB	Hard			
E:\S\Lavori	44%	2.00 GB	Hard			
E:\S\Coattiva	7%	40.0 GB	Hard			
E:\S\OrgaSapna	9%	1.00 GB	Hard			
E:\Condivisa_Sapna	98%	20.0 GB	Hard			
E:\S\Segreteria	4%	1.00 GB	Hard			
E:\S\Directory Comune Contratti	86%	10.0 GB	Hard			
E:\S\Ammacquisti	0%	1.00 GB	Hard			
E:\S\Help	0%	1.00 GB	Hard			
E:\S\Amministrazione	78%	70.0 GB	Hard			
E:\S\Flussi	79%	60.0 GB	Hard			
E:\S\Affari Generali	83%	30.0 GB	Hard			
E:\S\Servizi Tecnici	54%	30.0 GB	Hard			
E:\S\Segreteria Tecnica	46%	70.0 GB	Hard			
E:\S\Acquisti	71%	12.0 GB	Hard			
E:\S\Contratti	80%	12.0 GB	Hard			
E:\S\SW	72%	5.00 GB	Hard			
E:\S\Contabilita Industriale	50%	5.00 GB	Hard			
E:\scan_rete	0%	5.00 GB	Hard			
Source Template: 30_GB_template (6 items)						
E:\S\Dt_Segreteria _Tecnica	33%	10.0 GB	Hard	30_GB_template	Yes	
E:\S\DOC_LEGALI_CONDIVISA	36%	30.0 GB	Hard	30_GB_template	No	
E:\S\Contabilita	35%	30.0 GB	Hard	30_GB_template	No	
E:\S\Stir	52%	10.0 GB	Hard	30_GB_template	Yes	
E:\S\Personale	50%	10.0 GB	Hard	30_GB_template	Yes	
E:\S\ServizioPP	48%	30.0 GB	Hard	30_GB_template	No	

Figura 5

➢ Il server Backup ha funzione di storage per tutte le fonti dei backup che sono:
- File e cartelle dal file server
- DB file da server winwaste timbrature e protocollo facile.
  I DB server eseguono mediante script l'export dei dati direttamente negli share messi a disposizione sul server Backup, mentre per la componente file e cartelle viene utilizzato Cobian Backup nella versione gratuita.

- Il server Winwaste ha funzioni Applicative per il relativo software, raggiungibile da tutti i TMB, per la gestione del ciclo dei rifiuti.
- Il server Timbrature è relativo alla gestione dei marcatempo di tutti i presidi della SAPNA, sia quelli della sede centrale che dei TMB che delle discariche o siti remoti, i quali tramite collegamento VPN inviano al server i relativi dati delle timbrature del personale.
- Il Server Protocollo facile è solo per la consultazione dei vecchi protocolli, antecedenti la messa in esercizio del sistema Folium, (anno 2016) il db è in sola lettura.

8.4. Descrizione dell'infrastruttura di Sicurezza Informatica

Premesso che, le linee guida relative alla sicurezza aziendale attualmente implementate su tutti i sistemi del dominio Active Directory della S.A.P.NA. sono:

a) Ogni utente aziendale è provvisto di una username, password e indirizzo e-mail personale.

b) Le password di dominio per gli account utenti hanno le seguenti configurazioni:

- Scadenza ogni 90gg
- Lunghezza password almeno 10 caratteri
- Precedenti password ricordate: 10
- Complessità password abilitata
- Blocco dell'account dopo 10 tentativi falliti
- Sblocco dell'account dopo intervento Amministrativo

c) I tecnici delle ditte esterne che devono operare all'interno della rete aziendale vengono identificati già durante la creazione dell'identità di rete con il suffisso "guest" apposto al loro nome, in base alle informazioni ricevute dall'ufficio richiedente l'account viene generato con una scadenza pre-impostata e ricevono delle regole di password più restrittive, che sono:

- Scadenza ogni 60gg
- Lunghezza password almeno 14 caratteri
- Precedenti password ricordate: 24
- Complessità password abilitata
- Blocco dell'account dopo 5 tentativi falliti
- Sblocco dell'account dopo intervento Amministrativo

d) Nessuno degli account utenti del personale interno è membro dei gruppi amministrativi di sistema, solo specifici utenti del reparto ICT sono membri del gruppo Domain Admins, Enterprise Admins, e Local Administrators group

e) L'account Administrator locale è disabilitato, e viene creato un account di servizio con privilegi amministrativi locali per accedere in caso di evenienza sui sistemi.

f) L'accesso alle risorse di rete condivise avviene sempre tramite permessi espliciti, e sono deprecati tutti gli accessi mediante uso di gruppi dalla membership non gestibile quali:

- Everyone
- Authenticated Users
- Domain Users

8.4.1. Sicurezza dei dati, inclusi database, files, folders. Regole di *retention* dei dati e diagramma operativo.

Descrizione delle politiche di backup:

L'attuale configurazione dei backup dei dati prevede il seguente processo:

1) Ogni sistema di tipo Application server invia mediante servizio locale di backup o script i dati da esso gestiti a un *repository* di rete centrale che è il server in cloud SRV-BACKUP-01.

2) Nel caso dei documenti condivisi, sono abilitate sia sul server che ospita il servizio e sia sul NAS le funzioni di *shadow copy* dei dati, con *retention* di 1 mese.

3) Il server di backup, tramite il software Cobian Backup Free esegue il backup dei seguenti dati presenti sui server in cloud con una *retention* di 14 gg:

a) Cartelle contenenti i backup dei singoli db

b) Cartelle contenenti i backup delle cartelle condivise e dei files

Il design operativo è il seguente:

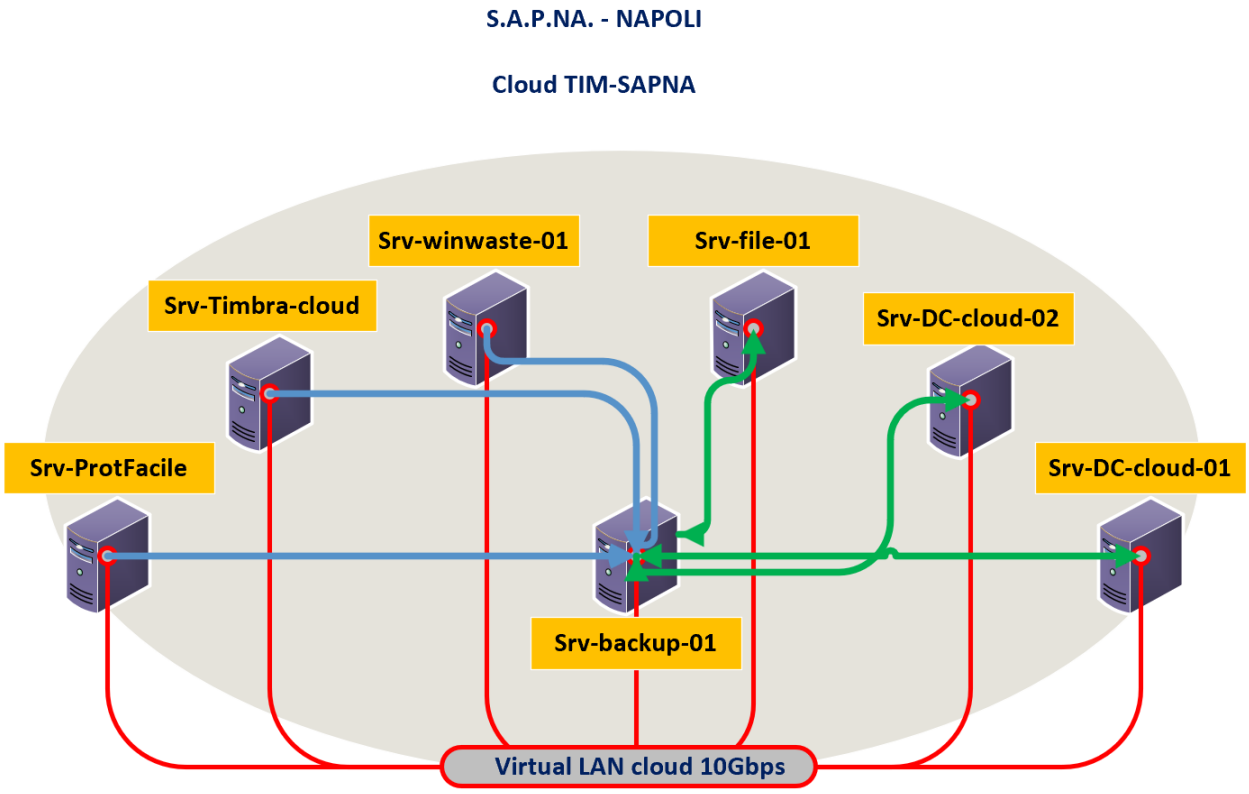


Figura 6

8.4.2. Sicurezza perimetrale e degli accessi. Apparati e Servizi presenti e diagramma operativo.

Per quanto riguarda i sistemi di sicurezza implementati al momento si evidenzia nella seguente tabella il tipo, la funzione e se in Alta Affidabilità (HA).

apparato	funzione	HA
Fortigate 81E v7.0.8	Firewall di rete perimetrale con funzionalità IPS / IDS e WAF abilitate. La sua funzione principale oltre a difendere la rete interna dal traffico dati proveniente da Internet è quella di filtrare il traffico web, inibendo l'accesso ai siti ed ai contenuti malevoli.	SI
Sophos Antivirus - InterceptX	Sistema Antivirus gestito mediante consolle in CLOUD Sohpos, il sistema è dotato di un'intelligenza artificiale basata sul deep learning presente in Intercept X che primeggia nel rilevare e bloccare i malware, anche mai visti prima. Agisce analizzando gli attributi dei file di centinaia di milioni di campioni per identificare le minacce senza doversi affidare alle firme.	SI

Tabella 4

Per quanto concerne la connettività, si precisa che tutti link di connessione della sede centrale di Napoli sono ridondati, sia a livello di apparati di connessione alla rete (routers e/o switches) sia dal punto del cablaggio, con cavi che seguono percorsi differenti e si attestano in centrali differenti.
Questo al fine di garantire la massima sicurezza possibile in caso di guasto.

9. Architettura di interconnessione

9.1. Sistema di connessione tra le sedi, le reti MPLS, VPN, CLOUD e INTERNET

Premesso che la S.A.P.NA. ha una rete distribuita su più siti, di cui i 4 connessi tra di loro in MPLS:

- Napoli, sede principale Uffici
- TMB Giugliano
- TMB Tufino
- Cloud TIM

a questi si aggiungono 13 siti remoti di stoccaggio dove sono presenti soprattutto dei rilevatori di presenza, i quali dialogano con la sede principale di Napoli, che è l'hub centrale di questa rete, mediante apposita VPN IPSec Always On.
La rete ha quindi un'architettura di tipo *hub-and-spoke*, dove la sede di Napoli è il punto centrale dove convergono tutte le connessioni, e al quale è attestato l'accesso ad Internet attraverso i firewall aziendali.
Le connessioni verso i diversi siti della SAPNA è quindi riassunta come segue:

Sede	Tecnologia di connessione	Connesso a:
Napoli	MPLS – Fibra	INTERNET - Sedi remote - TMB - Cloud
TMB Giugliano	MPLS	Sede di Napoli
TMB Tufino	MPLS	Sede di Napoli
Cloud TIM	MPLS	Sede di Napoli
Remoti (Discariche-Siti)	VPN IPSec over Internet	Sede di Napoli

Tabella 5

Il design operativo è il seguente:

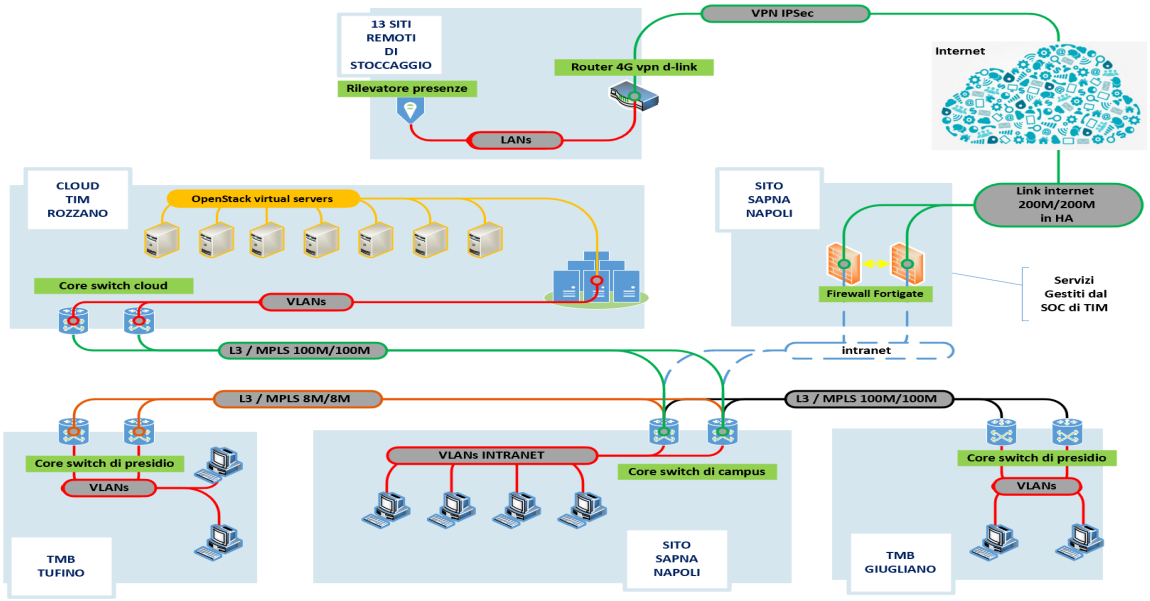


Figura 7

Il nodo principale di arrivo Telecom è ubicato nel rack gestore dati e telefonico del locale tecnico al 3° Piano, nel quale sono allocati i server, i patch panels, gli switch di distribuzione rete orizzontale dei locali del 3° Piano agli utenti, i collegamenti telefonici e i collegamenti in verticale con i locali tecnici del 2° Piano e del Piano Terra. Al punto di arrivo Telecom è predisposto anche un pannello FO per la connessione in fibra ottica di fornitura Telecom. Parimenti è connesso in verticale con cavo in fibra ottica il 3° Piano con il 2° Piano per il tramite di appositi pannelli di interconnessione tra i

rispettivi rack. Al 2° Piano, nel dedicato Locale Tecnico, è allocato un altro rack nel quale sono installati gli switch di distribuzione orizzontale rete dei locali del 2° Piano agli utenti, i collegamenti telefonici e i collegamenti in verticale provenienti dai locali tecnici del 3° Piano.
La distribuzione di rete dati sia per il 3° Piano, per il 2° Piano che per il Piano Terra, avviene a partire dagli switch singolarmente, a mezzo cavo in rame 4cp cat.6, direttamente dalla porta di uscita fino alla presa RJ45 dell'utente, senza interposizione di apparecchi o dispositivi intermedi. Le patch cord utilizzate per le connessioni dalla presa al PC e per le connessioni agli switch sono di tipo preformato.

9.2. Organizzazione logica di rete

La S.A.P.NA. S.p.A. ha realizzato un Dominio Microsoft Active Directory, aziendale, al fine di garantire un processo di "single sign-on" per tutti i dipendenti, previa migrazione di tutti i profili desktop presenti nei singoli PC in uso agli operatori. L'utilizzo di tale scelta assicura anche la scalabilità del sistema e l'implementazione di nuove caratteristiche e miglioramenti. I firewall sono assicurati da Telecom a monte, inclusi nel contratto di connessione in fibra ottica. L'accesso da ogni singolo PC inserito nel dominio aziendale è effettuato per il tramite di una interfaccia unica per login personalizzata con inserimento di username e password di accesso che identificano univocamente l'utente e la postazione di lavoro. Il sistema è in grado di tracciare gli accessi dalle singole postazioni di lavoro per tipologia di utente, inclusi gli accessi con credenziali di amministratore di sistema.
L'assegnazione degli indirizzi IP di rete è di tipo automatico (DHCP). Tale servizio in aggiunta al servizio di controllo degli accessi di rete (NPS) seleziona per il tramite di Certificati locali (CA Stand Alone) i computer che dialogano in rete.

10. Sicurezza Informatica: note generali

L'informazione è classificata come un bene aziendale e la maggior parte delle informazioni sono custodite su supporti informatici, siano essi di tipo fisso o mobile. Nell'ambito delle varie aree aziendali, ogni singola unità deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento ed evoluzione.
E' pertanto necessario provvedere ad impedire l'accesso ai dati presenti presso la rete aziendale non solo agli utenti non autorizzati, ma anche a soggetti con autorizzazione limitata a talune operazioni, per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati o cancellati. Le violazioni possono essere molteplici:

- tentativi non autorizzati di accesso a zone riservate,
- furto di identità digitale o di file riservati,
- utilizzo di risorse che l'utente non dovrebbe potere utilizzare ecc.
- guasti tecnici hardware, software, supporti;
- penetrazione estranea nelle reti di comunicazione;
- errori umani;

E' necessario altresì anche prevenire eventuali situazioni di "Denial of service" (DoS), ovvero attacchi sferrati al sistema (sia dall'esterno che dall'interno) con l'obiettivo di renderne inutilizzabili alcune risorse in modo da danneggiare gli utenti del sistema (ad esempio diffusione di criptovirus o di trojan distruttivi di file testo, etc.).
Pertanto si provvede alla protezione del dato attuando misure di sicurezza attiva e sicurezza passiva. Per sicurezza passiva (sicurezza fisica) normalmente si intendono le tecniche e gli strumenti di tipo difensivo, ossia quel complesso di soluzioni tecnico-pratiche il cui obiettivo è quello di impedire che utenti non autorizzati possano accedere a risorse, sistemi, impianti, informazioni e dati di natura riservata.
Il concetto di sicurezza passiva è quindi molto generale: ad esempio, per l'accesso fisico a locali protetti, l'utilizzo di porte di accesso blindate, congiuntamente all'impiego di sistemi di identificazione personale, sono da considerarsi componenti di sicurezza passiva.
Diversamente, per sicurezza attiva (sicurezza dati e programmi) si intendono, invece, tutte quelle tecniche e gli strumenti mediante i quali le informazioni ed i dati di natura riservata sono resi intrinsecamente sicuri, proteggendo gli stessi sia dalla possibilità che un utente non autorizzato possa accedervi (confidenzialità), sia dalla possibilità che un utente non

autorizzato possa modificarli (integrità). Rientrano in questa tipologia misure di sicurezza previste sia con strumenti hardware che software.
Sicurezza passiva e quella attiva sono tra loro complementari ed entrambe indispensabili per raggiungere il desiderato livello di sicurezza di un sistema.

11. Sicurezza Informatica: principali cause di perdita di dati

Le cause di probabile perdita di dati nei sistemi informatici possono essere riconducibili a due tipologie, quali a) eventi indesiderati e b) eventi accidentali. Ovviamente gli eventi non desiderati sono tutti quelli dovuti ad attacchi malevoli, ingressi non autorizzati o inconsapevoli di elementi degradanti, etc. mentre gli eventi accidentali non riguardano attacchi malevoli, ma fanno riferimento a eventi causati accidentalmente dall'utente stesso, tipo: uso difforme dal consigliato di un qualche sistema, incompatibilità di parti hardware, guasti imprevisti, etc.
In ogni caso di avveramento di essi, comunque viene compromessa la sicurezza del sistema, soprattutto in termini di disponibilità, con rallentamento delle attività e danni che possono essere, in taluni casi, di grave entità.
Per far fronte a tali evenienze, specie se derivanti da possibili guasti o danni fisici, molte volte si opera in un contesto di ridondanza degli apparati (es. server cluster) ovvero con sistemi distribuiti all'interno di piani di disaster recovery che, assicurando la tolleranza ai guasti (fault tolerance), garantiscano affidabilità e disponibilità cioè il business continuity del sistema informatico e dell'azienda oppure agendo in maniera preventiva tramite piani di disaster prevention.
Gli effetti degli attacchi pericolosi in quanto tali, consistono non solo nella presa di possesso di requisiti, dati e servizi altrui, ma anche causa all'utente cosiddetto "derubato" una sorta di insicurezza a far fede sui sistemi informatici, soprattutto se aziendali e potrebbero costituire causa di contenzioso.

12. Misure di prevenzione e protezione del dato informatico

Le norme riportate in questa sezione sono finalizzate ad aumentare la sicurezza dei singoli sistemi informatici utilizzati per il trattamento dei dati. Il rispetto di tali norme garantisce anche che non vengano compromesse le misure di sicurezza del sistema informativo ad opera di un utente regolarmente autorizzato, che, inconsapevolmente, adotti comportamenti in grado di violare l'integrità del sistema (installazione inconsapevole di virus o di "trojan horse"). Gli utenti non devono, altresì, con qualunque mezzo, modificare le configurazioni hardware e software. Tale azione è prerogativa dell'Amministratore di Sistema e/o di suoi incaricati.
I Responsabili delle varie aree aziendali dovranno:

- assicurare che gli utenti non installino sulla postazione di lavoro programmi non attinenti alle attività di ufficio, ovvero programmi senza la preventiva autorizzazione;
- qualora non siano in grado di apprezzare l'impatto dei programmi per i quali si è chiesta l'installazione, dovranno coordinarsi con il Titolare del Trattamento per concordare la linea di condotta.
- garantire che gli incaricati dell'amministrazione di sistema provvedano all'aggiornamento, con cadenza almeno mensile, del software riferito alla sicurezza applicabile alla versione di sistema operativo.

12.1. Protezione da virus informatici

I virus informatici rappresentano una delle minacce principali per la sicurezza dei sistemi informativi e dei dati in esso presenti. Un virus informatico, come è noto, può modificare e/o cancellare i dati in esso contenuti, compromettere la sicurezza e la riservatezza di un intero sistema informativo, rendere indisponibile tutto o parte del sistema, compresa la rete di trasmissione dati. Al fine di non aumentare il livello di rischio di contaminazione da virus è opportuno che Responsabili ed incaricati provvedano a:

1) accertarsi che sul computer sia sempre operativo il programma antivirus aggiornato e con la funzione di monitoraggio attiva;
2) sottoporre a controllo, con il programma installato sul proprio p.c., tutti i supporti di provenienza esterna prima di eseguire i files in esso contenuti;

3) accertarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; nel caso che il mittente dia origine a dubbi, cancellare direttamente il messaggio senza aprire gli allegati;

4) non condividere con altri computer il proprio disco rigido;

5) non scaricare da Internet programmi o file non inerenti l'attività lavorativa o comunque sospetti.

12.2. Back-up dei dati

Gli incaricati che trattano i dati sui propri p.c. non collegati in rete, o per i quali non sono previsti back-up centralizzati, devono provvedere al back-up dei dati almeno mensilmente. Per Backup si intende il salvataggio dei dati di interesse in copie di sicurezza da effettuarsi periodicamente su CD o altri supporti. I supporti di back-up devono essere custoditi in luogo sicuro e ad accesso controllato. In occasione di ogni back-up, deve preliminarmente accertarsi l'esito positivo della procedura nonché disporsi la distruzione del precedente supporto. Tutti i Responsabili verificano la puntuale osservanza di siffatta prescrizione.

12.3. Utilizzo della rete Internet

Il sistema informativo aziendale ed i dati in esso contenuti possono subire gravi danneggiamenti per un utilizzo improprio della connessione alla rete Internet, anche in conseguenza della diffusione di virus informatici o accessi non autorizzati. I Responsabili delle singole aree operative aziendali vigilano che gli utenti utilizzino la connessione Internet esclusivamente per lo svolgimento dei propri compiti istituzionali, non diffondano messaggi di posta elettronica di provenienza dubbia, non utilizzino la casella postale assegnata per fini privati e personali e che non si avvalgano di servizi di comunicazione e condivisione di files (condivisione P2P "peer-to-peer"). È, inoltre, vietato effettuare il download e l'installazione di programmi dalla rete Internet, a meno che non si abbia l'esplicita autorizzazione da parte dell'amministratore di sistema o che sia l'operatore autorizzato ad eseguirlo previa informazione al Responsabile del Trattamento.

12.4. Sanzioni per inosservanza delle norme

Le istruzioni riportate nel presente documento integrano elementi di valutazione della condotta del lavoratore. La violazione delle prescrizioni contenute può generare, oltre che responsabilità penali e civili, l'irrogazione di sanzioni disciplinari ai sensi della normativa legalmente prevista ed, ovviamente, in considerazione della gravità della condotta. Queste regole generali vanno applicate da tutte le categorie di Incaricati.

13. Servizio di Help Desk Aziendale

Ogni singola postazione di lavoro "utente" dotata di PC, di collegamento alla rete dati comune e inserita nel dominio aziendale, ha nelle proprie disponibilità un'applicazione, con collegamento posto sul desktop del PC, per il tramite della quale l'utente potrà ricorrere alla richiesta di assistenza informatica (Vedi **Allegato 2**: Servizio di Help Desk).

La richiesta di assistenza avverrà per il tramite di password che sarà inserita dall'utente all'atto dell'avviamento dell'applicazione nell'apposito campo generato da quest'ultima. La password dovrà essere composta da almeno 6 caratteri alfabetici e/o numerici ed avrà caratteristiche di servizio, ovvero di temporaneità e non ripetibilità. Non dovrà essere fornita, per nessun motivo, la propria password di accesso al dominio aziendale.

La password temporanea sarà ricevuta dal preposto che provvederà a contattare l'utente richiedente. In ogni caso, per motivi di sicurezza, il preposto all'help desk durante il contatto telefonico con l'utente provvederà a registrare l'identità dello stesso, la postazione interessata, la data e l'ora della richiesta di assistenza.

L'utente, una volta disponibile in modalità di assistenza, potrà disporre di due possibilità, da scegliere secondo la gravità del guasto o del problema rilevato, ovvero:

A) di lasciarsi guidare telefonicamente per la risoluzione del problema, agendo in prima persona sotto la guida dell'help desk, fino alla soluzione del problema;

B) di fare agire direttamente l'helper in remoto sul proprio PC seguendo le operazioni dello stesso a video, fino alla soluzione del problema.

A fine sessione di intervento la postazione PC dell'utente sarà ripristinata nel suo stato di funzionamento normale.

14. Disposizioni Organizzative in ordine alla sicurezza informatica

Si riporta in corsivo in versione integrale la Disposizione Organizzativa D.O. 005 del 21.06.2016 che regola, per tutto il personale dipendente, l'utilizzo delle apparecchiature e delle attrezzature aziendali:

Premessa: *Nell'ambito dell'espletamento delle attività istituzionali svolte dalla SAPNA SpA, il personale in forza alla sede operativa di Via Ponte dei Francesi, 37/E, ai Siti e Discariche ed agli Impianti STIR, in ordine alle rispettive competenze, è dotato di apparecchiature, di attrezzature, strumentazioni, software e sistemi che contribuiscono all'esecuzione delle dette attività secondo criteri di qualità, economicità, rapidità ed efficacia, nel rispetto delle Procedure Aziendali, della Disciplina Aziendale RE 05.2014 ed. Aprile 2014, nonché da quanto previsto dal CCNL di categoria e ss. e dalla Normativa Legale vigente, al fine di raggiungere gli obiettivi e gli scopi statutari. Le apparecchiature, attrezzature, strumentazioni, software e sistemi in dotazione, intesi anche quali impiantistica fissa e mobile di rete dati e telefonica, sono di proprietà di S.A.P.NA. S.p.A. che è, nel caso di software, anche intestataria della licenza d'uso;*

1.0 *Tutto il personale che utilizza apparecchiature e/o attrezzature aziendali o quanto altro previsto in premessa, è tenuto ad utilizzare le stesse al meglio possibile, durante l'orario di lavoro stabilito, ad averne cura, e a servirsi delle stesse per il tempo strettamente necessario all'attività assegnata, prevista dal proprio ruolo e dalla propria mansione. Una volta eseguite le attività di competenza, l'apparecchiatura dovrà essere spenta – se non altrimenti utilizzabile per diversa disposizione – e la strumentazione o le attrezzature riposte e adeguatamente conservate per il riutilizzo. Nel caso di eventuali guasti o malfunzionamenti, questi dovranno essere segnalati al rispettivo Responsabile che provvederà alle azioni consequenziali, sulla base di quanto indicato dall'utente. Per motivi di sicurezza della persona e di protezione dei dati, è inoltre tassativamente vietato al personale non autorizzato l'accesso ai locali tecnici in cui sono allocati i quadri elettrici, gli armadi rack di rete dati, gli switch di rete e gli attestaggi telefonici;*

2.0 *Per quanto riguarda, nello specifico, l'uso di Personal Computer aziendali, incluso portatili ed eventuali tablet, o similari in dotazione - a qualsiasi titolo - al personale dipendente della S.A.P.NA. S.p.A., questi dovranno essere connessi alla presa di rete dati aziendale direttamente, per il tramite dell'apposito cavo in dotazione e privi di interfacce, filtri, switch, e/o apparecchiature di ogni genere e tipo. E' altresì vietato l'uso di CD scrivibili, di chiavi USB, dischi esterni HDD di ogni tipo, telefoni cellulari, switch di rete secondari, hub, dispositivi wi-fi e similari, connessi ai Personal Computer aziendali e/o connessi con qualsiasi mezzo o interfaccia alla rete dati aziendale. L'utilizzo di prese di rete dati aziendali diverse da quelle assegnate all'utente per default, oppure di qualsivoglia apparecchiatura o elemento – inclusi quelli precedentemente elencati - che non siano stati previsti o installati dal personale preposto, a qualsiasi titolo utilizzati, e non preventivamente autorizzati per iscritto dal Responsabile Affari Generali, sarà considerata violazione del presente disposto, segnalata all'Ufficio Amministrazione del Personale e costituirà elemento di contestazione e provvedimento disciplinare;*

3.0 *Per quanto riguarda, nello specifico, l'utilizzo del collegamento a rete di accesso pubblico (internet), è fatto divieto al personale dipendente la connessione ai siti di social network, a siti non autorizzati quali quelli offensivi del decoro e del buon costume, o lesivi del rispetto, della professionalità e dell'onore della persona, nonché a siti web di vendita, giochi e scommesse. L'utilizzo di qualsiasi indirizzo di posta elettronica aziendale va effettuato per i soli scopi societari. Non è consentito utilizzare il proprio indirizzo di posta elettronica aziendale, per scopi diversi dai compiti istituzionalmente previsti. Se a seguito di verifica ispettiva venisse rilevata attività riconducibile alla violazione dei divieti anzidetti da parte dell'utente, l'esito della verifica sarà segnalato all'Ufficio Amministrazione del Personale e sarà elemento di contestazione e provvedimento disciplinare.*

4.0 *La validità della presente disposizione è a partire dalla data odierna. Tutti i soggetti i dipendenti e le aree aziendali interessate sono tenuti all'osservanza ed all'applicazione della presente disposizione ed a contribuire, per le specifiche aree di competenza, al rispetto dell'applicazione di quanto richiesto. Distribuzione: Direzione Tecnica, Ufficio Tecnico, Ufficio Amministrazione del Personale, Ufficio Amministrazione e Finanza, Gare e Contratti, Legale e Societario[2], Flussi, Segreteria Direzione[3], Segreteria Tecnica, STIR[4] Giugliano, STIR Tufino, Siti e Discariche, Protocollo (S.A.P.NA. S.p.A.), Organismo di Vigilanza (S.A.P.NA. S.p.A.),Collegio Sindacale (S.A.P.NA. S.p.A.).*

15. Richiami a disposizioni e leggi in materia penale e di protezione dati personali

15.1. Richiami al Codice Penale

Articolo 615 ter Accesso abusivo ad un sistema informatico o telematico

[5]Chiunque abusivamente si introduce in un sistema informatico o telematico[6] protetto da misure di sicurezza[7] ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

[2] oggi unità operative dell'Ufficio Affari Generali
[3] oggi unità operativa dell'Ufficio Affari Generali
[4] oggi Impianti TMB
[5] Il presente articolo è stato aggiunto dall'art. 4, della l. 23 dicembre 1993, n. 547.
[6] Viene sanzionato l'accesso virtuale, che quindi non comporta condotte di aggressione fisica al sistema cui si accede a distanza su reti telematiche.
[7] La presenza di un sistema di protezione da accessi abusivi implica un'espressa volontà contraria del soggetto di far accedere altri al proprio sistema.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;
2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;
3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

Articolo 615 quater Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

[8]Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo[9], è punito con la reclusione sino a un anno e con la multa sino a cinquemilacentosessantaquattro euro.

La pena è della reclusione da uno a due anni e della multa da cinquemilacentosessantaquattro euro a diecimilatrecentoventinove euro se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617quater.

Articolo 615 quinquies Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico

[10]Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici[11], è punito con la reclusione fino a due anni e con la multa sino a euro 10.329.

15.2. Abstract dal Codice in materia di protezione dei dati personali

Allegato B.

Disciplinare tecnico in materia di misure minime di sicurezza (Artt. da 33 a 36 del Codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo

[8] Il presente articolo è stato aggiunto dall'art. 4, della l. 23 dicembre 1993, n. 547.
[9] Si ritiene che tra le condotte perseguite rientrino anche quella consistente nell'attivazione di un telefono cellulare clonato su un numero intesto ad altro soggetto, nonchè quella di clonazione dei decoder necessari per la ricezione di determinati programmi televisivi trasmessi via satellite.
[10] Il presente articolo è stato aggiunto dall'art. 4, della l. 23 dicembre 1993, n. 547 e modificato dalla l. 18 marzo 2008, n. 48.
[11] Si tratta di un reato di pericolo quindi per integrare il reato non è richiesto che si verifichi il danneggiamento o l'interruzione, essendo sufficiente la mera elaborazione di un sistema, apparecchiatura o programma idoneo a creare il rischio di un danneggiamento.

dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

---*Omissis*---

<u>Ulteriori misure in caso di trattamento di dati sensibili o giudiziari</u>

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

---*Omissis*---

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Violazione dei dati personali

Art. 32-bis Adempimenti conseguenti ad una violazione di dati personali [12]

1. In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione al Garante.

2. Quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza del contraente o di altra persona, il fornitore comunica anche agli stessi
senza ritardo l'avvenuta violazione.

3. La comunicazione di cui al comma 2 non é dovuta se il fornitore ha dimostrato al Garante di aver utilizzato misure tecnologiche di protezione che rendono i dati inintelligibili a chiunque non sia autorizzato ad accedervi e che tali misure erano state applicate ai dati oggetto della violazione.

4. Ove il fornitore non vi abbia già provveduto, il Garante può, considerate le presumibili ripercussioni negative della violazione, obbligare lo stesso a comunicare al contraente o ad
altra persona l'avvenuta violazione.

5. La comunicazione al contraente o ad altra persona contiene almeno una descrizione della natura della violazione di dati personali e i punti di contatto presso cui si possono ottenere
maggiori informazioni ed elenca le misure raccomandate per attenuare i possibili effetti pregiudizievoli della violazione di dati personali. La comunicazione al Garante descrive,
inoltre, le conseguenze della violazione di dati personali e le misure proposte o adottate dal fornitore per porvi rimedio.

6. Il Garante può emanare, con proprio provvedimento, orientamenti e istruzioni in relazione alle circostanze in cui il fornitore ha l'obbligo di comunicare le violazioni di dati
personali, al formato applicabile a tale comunicazione, nonchè alle relative modalità di effettuazione, tenuto conto delle eventuali misure tecniche di attuazione adottate dalla
Commissione europea ai sensi dell'articolo 4, paragrafo 5, della direttiva 2002/58/CE, come modificata dalla direttiva 2009/136/CE.

7. I fornitori tengono un aggiornato inventario delle violazioni di dati personali, ivi incluse le circostanze in cui si sono verificate, le loro conseguenze e i provvedimenti adottati per
porvi rimedio, in modo da consentire al Garante di verificare il rispetto delle disposizioni del presente articolo. Nell'inventario figurano unicamente le informazioni necessarie a tal
fine.

[12] Articolo inserito dall'art. 1, comma 3, del decreto legislativo 28 maggio 2012, n. 69.

8. Nel caso in cui il fornitore di un servizio di comunicazione elettronica accessibile al pubblico affidi l'erogazione del predetto servizio ad altri soggetti, gli stessi sono tenuti a comunicare al fornitore senza indebito ritardo tutti gli eventi e le informazioni necessarie a consentire a quest'ultimo di effettuare gli adempimenti di cui al presente articolo.

<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<FINE>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>