

Logo/ragione sociale

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto in conformità al D. Lgs. n. 196 del 30 Giugno 2003 "Codice in materia di protezione dei
dati personali"

Versione 00 del

La direzione: _____

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

Indice

COPERTINA	1
INDICE	2
CAPITOLO I	3
NOTE PRELIMINARI DEL PIANO PER LA SICUREZZA	
CAPITOLO II	24
IL PIANO DI SICUREZZA DI NOME AZIENDA	
CAPITOLO III	29
DESCRIZIONE DELL'ELENCO DEI TRATTAMENTI ELETTRONICO DEI DATI PERSONALI	
CAPITOLO IV	30
DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'	
CAPITOLO V	33
MISURE DI SICUREZZA SU AREE E LOCALI	
CAPITOLO VI	36
MISURE DI SICUREZZA SULL'INTEGRITA' DEI DATI	
CAPITOLO VII	42
CRITERI DA ADOTTARE PER LA CIFRATURA E PER LA SEPARAZIONE DI DATI PERSONALI RIGUARDANTI LO STATO DI SALUTE E LA VITA SESSUALE DAGLI ALTRI DATI PERSONALI DELL'INTERESSATO	
CAPITOLO VIII	45
CRITERI DA ADOTTARE E DELLE MODALITA' PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO	
CAPITOLO IX	46
CRITERI DA ADOTTARE PER GARANTIRE L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTO DI DATI PERSONALI AFFIDATI, IN CONFORMITA' AL CODICE, ALL'ESTERNO DELLA STRUTTURA DEL TITOLARE	
CAPITOLO X	47
PIANO DI FORMAZIONE	
CAPITOLO XI	48
VERIFICA DEL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA	

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CAPITOLO I

NOTE PRELIMINARI DEL PIANO PER LA SICUREZZA

1.1. DESCRIZIONE AZIENDALE

Descrivere brevemente l'azienda, struttura, nr dipendenti, tipo di attività, nr sedi, eccc

1.1.1. STRUTTURA DEL SISTEMA INFORMATICO AUTOMATIZZATO DI Nome azienda

Il sistema informatico di Nome azienda si compone di:

- nr x personal computer;
- nr x personal computer server;
- nr sistema di rete diretto via cavo;
- nr x stampanti, di cui x multifunzione ed x laser, ecc;
- nr gruppo di continuità;
- nr eccc

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CAPITOLO II

IL PIANO DI SICUREZZA DI NOME AZIENDA

2.1. ANALISI DELLE RISORSE DI NOME AZIENDA

LINEE GUIDA PER L'UTILIZZO DELLE RISORSE INFORMATICHE ED IL TRATTAMENTO DEI DATI PERSONALI

L'articolo 34 del D. Lgs. 196/2003 prevede, nel caso di trattamento di dati sensibili e giudiziari effettuati con strumenti elettronici, la predisposizione e l'aggiornamento del Documento Programmatico della Sicurezza.

Tale documento contiene:

ELENCO DEI TRATTAMENTI DI DATI PERSONALI

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

Titolare del trattamento

Responsabile del trattamento

Incaricati del trattamento

Preposto alla custodia della parola chiave

Incaricato alla manutenzione

Lettera incarico responsabile del trattamento

Lettera incarico preposto alla parola chiave

Lettera incarico incaricato al trattamento

Lettera incarico incaricato alla manutenzione

ANALISI DEI RISCHI E DELLE MINACCE

Distruzione o perdita

Accesso non autorizzato

Trattamento non conforme alle finalità della raccolta

MISURE DI SICUREZZA SU AREE E LOCALI

Protezione locali e modalità di accesso

Procedure organizzative e di controllo

MISURE DI SICUREZZA SULL'INTEGRITA' DEI DATI E CRITERI E PROCEDURE PER LA SICUREZZA DI
TRASMISSIONE DEI DATI – TRASMISSIONE TELEMATICA

Individuazione dei dati e procedure di controllo

Modalità di protezione dei dati

Procedure di sicurezza per l'integrità dei dati

Tecniche e modalità procedurali e organizzative

Modalità di accesso

Personale autorizzato

Tipologia dei dati trasmessi

Modalità di trasmissione e protezione

Procedure di controllo e autorizzazione

Tecniche e modalità organizzative

Personale autorizzato

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CRITERI DA ADOTTARE PER LA CIFRATURA O PER LA SEPARAZIONE DI DATI PERSONALI RIGUARDANTI LO STATO DI SALUTE E LA VITA SESSUALE DAGLI ALTRI DATI PERSONALI DELL'INTERESSATO

Procedure per la cifratura e/o la separazione di dati personali riguardanti la salute e la vita sessuale dagli altri dati personali

Tecniche e modalità organizzative

Personale autorizzato

Se applicabile, altrimenti punto non applicabile

CRITERI DA ADOTTARE E DELLE MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

Procedure di ripristino a seguito di distruzione e/o danneggiamento

Tecniche e modalità organizzative

Personale autorizzato

CRITERI DA ADOTTARE PER GARANTIRE L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTI DI DATI PERSONALI AFFIDATI, IN CONFORMITÀ AL CODICE, ALL'ESTERNO DELLA STRUTTURA DEL TITOLARE

Tipologia dei dati trasmessi

Modalità di trasmissione e protezione

Procedure di controllo e autorizzazione

Tecniche e modalità organizzative

Personale autorizzato

Se applicabile altrimenti punto non applicabile

PIANO DI FORMAZIONE

Soggetti interessati

Contenuti, modalità e documentazione

VERIFICA DEL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

Procedure per la verifica del documento

Tecniche e modalità organizzative

Personale incaricato

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

2.3. ELENCO PROCEDURE GESTIONALI

UBICAZIONE ARCHIVI CARTACEI E SUPPORTI MAGNETICI

NOME AZIENDA	ARCHIVIO CARTACEO DIPENDENTI	ARCHIVIO CARTACEO CLIENTI	ARCHIVIO CARTACEO FORNITORI	BACKUP DATI CONTABILITA'	BACK UP DATI RETE SERVER

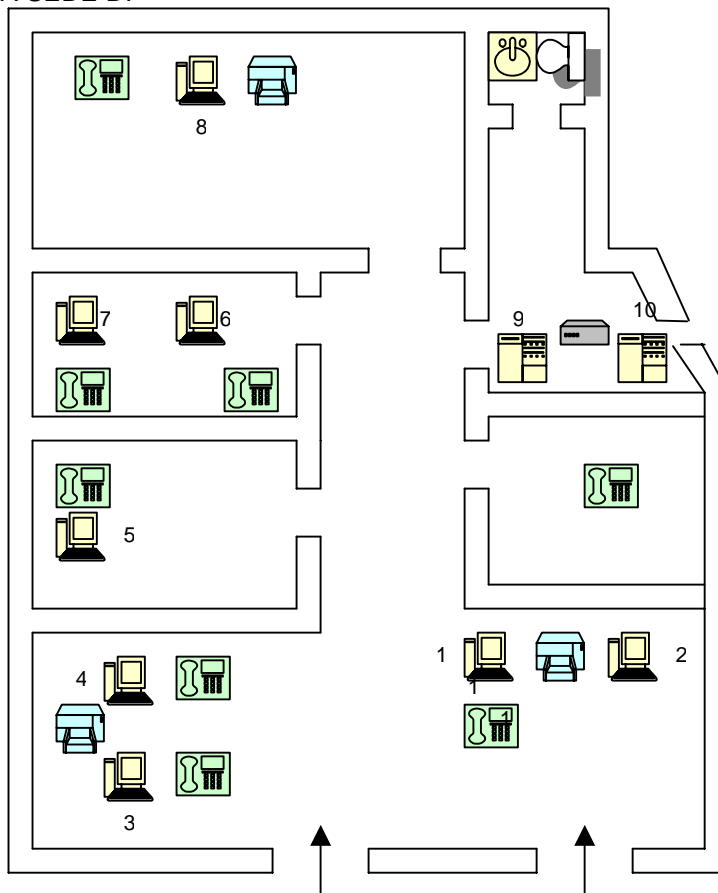
2.4. ARCHIVI INFORMATICI

SEDE	INDIRIZZO	CAP	CITTA'	ARCHIVIO INFORMATICO

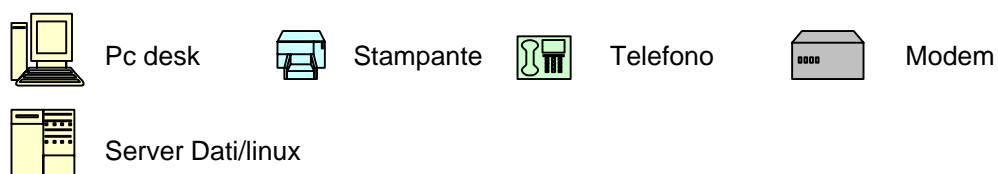
2.5. COLLOCAZIONE FISICA DELL'IMPIANTO INFORMATICO

- PLANIMETRIA SEDE DI

ESEMPIO



Legenda:



Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

2.6. CLASSIFICAZIONE O NATURA DEI DATI TRATTATI, SUDDIVISI PER SERVIZI

2.6.1. AREA SEGRETERIA ESEMPIO

DEFINIZIONE SERVIZIO	CLASSIFICAZIONE O NATURA DEI DATI TRATTATI		ARCHIVIAZIONE	
	PERSONALI	SENSIBILI	CARTACEA	INFORMATICA
<ul style="list-style-type: none"> - Portare a compimento le linee strategiche di gestione dell'azienda dettate dalla direzione.; - Gestione amministrativa dell'azienda; - gestione del personale; - gestione degli acquisti; - accoglienza dei soggetti esterni (clienti, fornitori, ecc.); - garantire i flussi ed il rispetto delle procedure previste per la corrispondenza dell'azienda, - garantire, nel rispetto delle procedure interne e delle normative fiscali, civilistiche e contrattualistiche, l'amministrazione contabile; - il rispetto delle scadenze contrattuali e fiscali; - la gestione degli adempimenti connessi al personale dipendente; - il reporting aggiornato alla direzione; - l'attività di segreteria amministrativa; - un controllo di gestione sull'attività dell'azienda - elaborazione dati contabili e fiscali nel rispetto delle normative fiscali. 	<ul style="list-style-type: none"> - Tutti i dati anagrafici; indirizzi e recapiti telefonici di dipendenti, clienti, fornitori e collaboratori; dati bancari e contabili e fiscali di dipendenti / collaboratori, fornitori e clienti. 	<ul style="list-style-type: none"> - Dati relativi ai certificati di malattia / infortunio per i dipendenti/clienti 	<ul style="list-style-type: none"> - Documentazione generale dei clienti; - Documenti fiscali. Dati fiscali e previdenziali dei dipendenti e clienti. - Documenti contrattuali; - Contratti collaboratori esterni. - Archiviati in armadi o cassette muniti di serratura presso i vari uffici. 	<ul style="list-style-type: none"> I dati personali e sensibili sono elaborati ed archiviati mediante i seguenti programmi: - Gestionale XXXX; - Microsoft Office;XP/NT/WINDOWS 2000; - X - Osra Veneto.

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

2.6.2. AREA DIREZIONE ESEMPIO

DEFINIZIONE SERVIZIO	CLASSIFICAZIONE O NATURA DEI DATI TRATTATI		ARCHIVIAZIONE	
	PERSONALI	SENSIBILI	CARTACEA	INFORMATICA
<ul style="list-style-type: none"> - Definire le linee strategiche di gestione dell'azienda.; - Attività consulenziale in materia 	<p>Tutti i dati anagrafici; indirizzi e recapiti telefonici di dipendenti, clienti, fornitori e collaboratori; dati bancari e contabili di dipendenti/collaboratori, fornitori ed enti.</p>	<ul style="list-style-type: none"> - Dati relativi ai certificati di malattia/infortunio per i dipendenti/clienti. - Dati relativi alle attività di accertamento, nei limiti delle proprie finalità istituzionali, con riferimento ai dati relativi ad esposti o petizioni per i clienti - Dati volti all'applicazione delle norme in materia di sanzioni e ricorsi, necessari per far valere il diritto di difesa anche da parte di un terzo per i clienti. - Dati rivolti a individuare lo stato di salute dei clienti. - Dati rivolti ad individuare le convinzioni filosofiche (obiezione di coscienza contro le armi). 	<ul style="list-style-type: none"> - Documenti contrattuali, libri sociali, atti societari, dei clienti; - Archiviati in armadi o cassette muniti di serratura presso i vari uffici. 	<p>I dati personali e sensibili sono elaborati ed archiviati mediante i seguenti programmi:</p> <ul style="list-style-type: none"> - Gestionale XXXX; - Microsoft Office;XP/NT/WINDOWS 2000; - Osra Veneto.

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

2.6.3. AREA AMMINISTRATIVA ESEMPIO

DEFINIZIONE SERVIZIO	CLASSIFICAZIONE O NATURA DEI DATI TRATTATI		ARCHIVIAZIONE	
	PERSONALI	SENSIBILI	CARTACEA	INFORMATICA
<ul style="list-style-type: none"> - Portare a compimento le linee strategiche di gestione dell'azienda dettate dalla direzione.; - Gestione amministrativa dell'azienda; - gestione del personale; - gestione degli acquisti; - accoglienza dei soggetti esterni (clienti, fornitori, ecc.); - garantire i flussi ed il rispetto delle procedure previste per la corrispondenza dell'azienda, - garantire, nel rispetto delle procedure interne e delle normative fiscali, civilistiche e contrattualistiche, l'amministrazione contabile; - il rispetto delle scadenze contrattuali e fiscali; - la gestione degli adempimenti connessi al personale dipendente; - il reporting aggiornato alla direzione; - l'attività di segreteria amministrativa; - un controllo di gestione sull'attività dell'azienda - elaborazione dati contabili e fiscali nel rispetto delle normative fiscali. 	<ul style="list-style-type: none"> - Tutti i dati anagrafici; indirizzi e recapiti telefonici di dipendenti, clienti, fornitori e collaboratori; dati bancari e contabili e fiscali di dipendenti / collaboratori, fornitori e clienti. 	<ul style="list-style-type: none"> - Dati relativi ai certificati di malattia / infortunio per i dipendenti/clienti 	<ul style="list-style-type: none"> - Documentazione generale dei clienti; - Documenti fiscali. Dati fiscali e previdenziali dei dipendenti e clienti. - Documenti contrattuali; - Contratti collaboratori esterni. - Archiviati in armadi o cassette muniti di serratura presso i vari uffici. 	<p>I dati personali e sensibili sono elaborati ed archiviati mediante i seguenti programmi:</p> <ul style="list-style-type: none"> - Gestionale XXXX; - Microsoft Office;XP/NT/WINDOWS 2000; - Osra Veneto.

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

2.7. MISURE DI ADEGUAMENTO

Procedendo all'incrocio tra dati trattati e tipologie di strumenti utilizzati per trattarli, si ottiene che la mappa delle categorie delle misure minime di sicurezza che devono essere adottate è la seguente (tabella 01):

LEGENDA:

A = archivi cartacei

c = dati comuni

B = PC in rete

s = dati sensibili

■ misure di sicurezza minime ed idonee adottate o in via di adozione da Nome azienda

Tabella 01

	A		B	
	c	s	c	s
MISURE MINIME DI SICUREZZA DI Nome azienda				
A – ADEMPIMENTI NELLA ATTRIBUZIONE DI RUOLI E COMPITI				
A1 – Usare in tutti i casi la forma scritta e fornire istruzioni dettagliate	■	■	■	■
B – PREVEDERE PROCEDURE PER LA CLASSIFICAZIONE DEI DATI				
B1 – Prevedere procedure per la classificazione dei dati trattati	■	■	■	■
C – PROCEDERE ALLA CREAZIONE E GESTIONE DI ARCHIVI FISICI				
C1 – Archivio ad accesso controllato – per i dati personali	■	■	■	■
D – INTRODURRE MISURE LOGICHE DI GESTIONE DEGLI ACCESSI				
D1 – Semplice attribuzione di parole chiave (<i>passwords</i>)			■	■
D2 – Attribuzione del codice identificativo personale			■	■
D3 – Autorizzazione all'accesso di dati particolari			■	■
E – INSTALLAZIONE DI SOFTWARE DI PROTEZIONE				
E1 – Installazione di software di protezione			■	■
F – CONTROLLO DEI SUPPORTI DI MEMORIZZAZIONE				
F1 – Procedure di controllo dei supporti di memorizzazione			■	■
G – DOCUMENTO PROGRAMMATICO DI SICUREZZA				
G1 – Analisi dei rischi	■	■	■	■
G2 – Protezione di aree e locali interessati dalle misure di sicurezza	■	■	■	■
G3 – Autorizzazione all'accesso delle persone ai locali e controllo	■	■	■	■
G4 – Assicurare l'integrità dei dati	■	■	■	■
G5 – Assicurare la sicurezza in caso di dati affidati all'esterno della struttura	■	■	■	■
G6 - Assicurare il ripristino della disponibilità dei dati a seguito di distruzione o danneggiamento			■	■
G7 – Assicurare la sicurezza nella trasmissione dei dati			■	■
G8 – Formazione degli incaricati del trattamento	■	■	■	■
G9 – Controllo generale periodico sullo <i>stato della sicurezza</i>	■	■	■	■
G10 – Redazione e revisione del Documento programmatico di sicurezza	■	■	■	■

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CAPITOLO III
DESCRIZIONE DELL'ELENCO DEI TRATTAMENTI INFORMATICO DEI DATI PERSONALI

DESCRIZIONE	DATI				
	PERSONALI	SENSIBILI	GIUZIARI	SALUTE	VITA SESSUALE
Soci	X	X	X		
Dipendenti	X				
Collaboratori	X				
Clienti	X	X	X	X	
Fornitori	X				

DESCRIZIONE DELL'ELENCO DEI TRATTAMENTI CARTACEO DEI DATI PERSONALI

DESCRIZIONE	DATI				
	PERSONALI	SENSIBILI	GIUZIARI	SALUTE	VITA SESSUALE
Soci	X	X	X	X	
Dipendenti	X			X	
Collaboratori	X				
Clienti	X	X	X	X	
Fornitori	X				

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CAPITOLO IV

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

4.1. CARICHE E RESPONSABILITA' DI NOME AZIENDA

APPROVATO DALL'ASSEMBLEA DEI SOCI DEL

4.1.1. Titolare del trattamento.

CARICHE E RESPONSABILITA'	DEFINIZIONE E COMPITI	NOMINATIVO PROPOSTO
TITOLARE DEL TRATTAMENTO	Si definisce titolare del trattamento, la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente, associazione od organismo cui oggettivamente competono le decisioni strategiche di fondo su come (modalità) e perché (finalità) raccogliere e trattare dati, nonché sull'organizzazione del trattamento e sulle risorse da dedicarvi, anche per garantire la sicurezza. Esso non può sottrarsi, anche se delega taluno o al limite tutti gli aspetti gestionali ad altri soggetti, al compito di vigilare sul fatto che le disposizioni sulla privacy vengano diligentemente rispettate e che le misure di sicurezza vengano attuate.	

4.1.2. Responsabile del trattamento.

RESPONSABILE DEL TRATTAMENTO	Si definisce responsabile del trattamento, la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente, preposta dal titolare del trattamento dei dati personali. Esso deve essere nominato tra i soggetti che per esperienza, capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Esso deve procedere al trattamento attendendosi alle istruzioni impartite dal titolare che, anche attraverso verifiche periodiche, deve vigilare sulla puntuale osservanza delle disposizioni e delle istruzioni impartite. Il responsabile del trattamento può essere più di uno.	
-------------------------------------	--	--

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

4.1.3. Incaricato del trattamento.

INCARICATO DEL TRATTAMENTO	Si definisce incaricato del trattamento, la persona incaricata per iscritto, di compiere le operazioni del trattamento dal titolare o dal responsabile, e che opera sotto la loro diretta autorità, la quale deve elaborare i dati personali ai quali ha accesso attendendosi alle istruzioni del titolare o del responsabile.	
-----------------------------------	--	--

4.1.4. Preposto alla parola chiave.

PREPOSTO ALLA PAROLA CHIAVE	Si definisce preposto alla parola chiave, il soggetto preposto alla custodia delle parole chiave (passwords), che consentono l'accesso agli elaboratori elettronici: tale figura deve essere nominata per iscritto da chi tratta i dati personali mediante l'uso degli elaboratori elettronici, se vi è più di un incaricato del trattamento e sono in uso più parole chiave per accedere a tali elaboratori. E' possibile nominare più di un preposto, il cui compito è di custodire la parola chiave (passwords) ed attribuirle agli incaricati del trattamento.	
------------------------------------	--	--

4.1.5. Incaricato alla manutenzione.

INCARICATO ALLA MANUTENZIONE	Si definisce come incaricato alla manutenzione, la persona fisica o giuridica che è incaricata per iscritto di compiere determinate operazioni di manutenzione hardware e software.	
-------------------------------------	---	--

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CAPITOLO V

MISURE DI SICUREZZA SU AREE E LOCALI

5.1. PROTEZIONE LOCALI E MODALITA' DI ACCESSO

La protezione delle aree ove vengono trattati e/o conservati i dati personali e sensibili è principalmente connessa con la sicurezza fisica dei locali rispetto alle risorse umane ivi impiegate, ed alle componenti materiali ed organizzative che costituiscono il sistema informativo aziendale.

Rispetto al problema, Nome azienda è venuta ad organizzare un servizio di protezione della sede dell'impresa implementato attraverso sistemi di sorveglianza diretta tramite il proprio personale dipendente. Sono state predisposte misure di controllo per l'ingresso nei locali ove sono trattate informazioni riservate e ci si è dotati di armadi e classificatori non facilmente accessibili e violabili da persone terze estranee all'organizzazione aziendale, ovvero da parte di clienti della stessa società, collocandoli in aree non accessibili direttamente al pubblico.

Le misure di sicurezza fisica adottate riguardano la sicurezza perimetrale degli uffici, dei supporti cartacei ed informatici, delle banche dati. Inoltre il controllo fisico sull'accesso ai locali è fatto mediante la richiesta dell'identificazione fisica di terzi o del personale non incaricato al trattamento, che potrà accedervi esclusivamente previa autorizzazione rilasciata dal personale incaricato.

Gli elaboratori e le banche dati sono installati all'interno degli uffici dove possono accedere e sono autorizzati ad essere presenti durante l'orario di lavoro gli incaricati del trattamento dei vari servizi e le persone autorizzate.

Alla sera, al termine dell'orario di lavoro la sede è chiusa a chiave. Dopo l'orario di apertura al pubblico la sede è accessibile solo dal personale incaricato.

In particolare si è ritenuto necessario ed opportuno riservare il possesso e l'utilizzo delle chiavi di accesso alla sede esclusivamente ai rispettivi incaricati al trattamento dei dati.

5.2. PROCEDURE ORGANIZZATIVE E DI CONTROLLO

L'analisi dei rischi si conclude con l'individuazione di tutte le possibili misure di sicurezza di natura fisica, logica ed organizzativa, che potrebbero essere adottate al fine di limitare l'entità del rischio.

E' quindi necessario, valutare l'esposizione al rischio e individuare le misure di sicurezza più opportune e necessarie da adottare.

La valutazione delle minacce e delle vulnerabilità prende in considerazione molte tipologie di potenziali problemi, ognuna delle quali interessa diverse parti del sistema informativo; esse devono essere raggruppate e poi correlate ai singoli beni informativi per classificare ed individuare la singola misura di sicurezza in relazione ai diversi servizi informativi.

In particolare il rischio connesso a specifica minaccia fisica ovvero a guasti tecnici delle apparecchiature viene affrontato attraverso una serie di misure di sicurezza che consentono di evidenziare le criticità in capo ai singoli beni ed al sistema informativo dell'organizzazione aziendale, in funzione degli impatti relativi agli elementi di integrità.

E' l'insieme delle misure fisiche di sicurezza che hanno il compito di prevenire ed impedire gli accessi fisici non autorizzati, danni o interferenze con lo svolgimento del trattamento dati. La protezione fisica delle aree e dei locali in cui sono situati gli elaboratori e le banche dati deve, quindi, essere attuata sia contro eventi dannosi imprevedibili, quali inondazioni, incendi, corti circuiti, sia contro tentativi di intrusione e furti.

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

A tal fine Nome azienda si è dotata delle seguenti procedure organizzative di controllo sul rischio fisico attraverso le seguenti misure di sicurezza fisiche:

- dispositivi antincendio;
- gruppo di continuità per tutelarsi da interruzioni od anomalie elettriche;
- accesso controllato agli armadi contenitori banche dati;
- climatizzazione naturale dei locali.

Contro la concreta minaccia di un'alterazione dei programmi e dati, per un qualche disastro naturale, sabotaggio, furto o sottrazione del dato trattato ed eventuale danneggiamento delle risorse informatiche e per essi il rischio di distruzione e/o perdita anche accidentale del dato personale trattato e l'accesso non autorizzato ci si garantisce dunque in primo luogo con la protezione fisica degli elaboratori e delle banche dati cartacee attraverso la predisposizione di luoghi e locali ad accesso controllato, nonché l'utilizzo di efficienti dispositivi antincendio, di continuità elettrica, di climatizzazione naturale dei locali.

Relativamente al primo aspetto, e cioè al rischio incendio/allagamento nei locali di Nome azienda esiste da tempo un sistema di installazione e manutenzione dei mezzi antincendio di proprietà aziendale in conformità alle prescrizioni antinfortunistiche e di prevenzione incendi vigenti, quali il D.P.R. 574/55 che prevede la revisione semestrale e l'apposizione di un cartellino di verifica con data e firma del tecnico preposto, previa sottoscrizione di idoneo contratto rinnovabile tacitamente di anno in anno con ditta specializzata esterna. La manutenzione dei mezzi antincendio comprende il controllo generale, la pulitura, la verifica dell'efficienza della carica e delle piccole riparazioni ed aggiustaggi eventualmente occorrenti, quando necessario collaudo degli estintori ad anidride carbonica (Co2).

I dati personali e sensibili vengono salvati su nastri magnetici e conservati in apposito armadio.

Per il pericolo di un allagamento, peraltro remoto, i computer sono stati posti in posizione rialzata da terra.

I pc e i server possono risentire di eventuali anomalie elettriche provenienti dai cavi di connessione quali reti elettriche, linee telefoniche, cavi seriali/paralleli, per questo motivo Nome azienda si è dotata anzitempo di un gruppo di continuità che ha lo scopo principale di fornire a pc e ai server energia elettrica continuativa nel caso questa venga a mancare, nonché di filtrare la corrente in ingresso da tutti i disturbi presenti sulla rete elettrica ed alimentare correttamente i pc e i server.

La protezione fisica delle banche dati contenute negli "armadietti/archivi" è attuata attraverso la chiusura a lucchetto a combinazione degli stessi alla fine di ogni giornata lavorativa, con custodia delle combinazioni in apposito luogo dotato anch'esso di chiave, a disposizione della direzione. Potranno accedere alle banche dati contenute negli armadietti solo gli incaricati del trattamento individuati con lettera d'incarico.

Quanto all'ultima misura di sicurezza posta in essere da Nome azienda, si è ritenuto opportuno preservare ogni tipo di supporto, sia cartaceo che informatico, da ogni possibile corruzione causata da eventuali sbalzi termici e di umidità dovuti al clima ed alle particolari condizioni di habitat operative presenti in ogni singolo ufficio, tramite climatizzazione naturale dei locali.

Tra le misure di sicurezza organizzative (che vanno ad affiancarsi ed integrarsi con le misure di sicurezza logiche e fisiche) Nome azienda è venuta a predisporre e a distribuire a tutto il proprio personale dipendente una istruzione operativa in merito all'utilizzo dei singoli supporti della banca dati ed alle modalità più efficienti ed ordinate di archiviazione dei dati personali raccolti e trattati.

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CAPITOLO VI

MISURE DI SICUREZZA SULL'INTEGRITA' DEI DATI

6.1. OPERAZIONI EFFETTUATE PER L'INDIVIDUAZIONE DEI DATI E PROCEDURE DI CONTROLLO PER LA SICUREZZA DEI TRASMISSIONE DEI DATI – TRASMISSIONE TELEMATICA

ANALISI RISCHI E MISURE DI SICUREZZA RELATIVE ALLE OPERAZIONI E COLLEGAMENTI EFFETTUATI

Presso la sede di Nome azienda sono presenti X elaboratori. Tutti i pc sono collegati in rete diretta via cavo ai server, compeltare a piacere.

Postazione nr x: l'elaboratore è utilizzato dal personale di segreteria, responsabile del corretto impiego, che è inoltre stato incaricato del trattamento dei dati personali ed autorizzato all'accesso per la gestione esclusiva delle operazioni connesse alla propria attività lavorativa. E' collegato in rete interna ed esterna mediante server. E' presente Windows 2000, programma gestionale, Winzip, Adobe Acrobat, completare. Non è possibile caricare programmi o aprire file da supporti esterni quali floppy disk o cd rom. Completare a piacere

Operazioni attuate	Valutazione dei rischi	Misure di protezione e sicurezza
Elaborazione testi, tabelle di calcolo, fatturazione clienti. Sono trattati dati personali dei clienti mediante software specifico.	Quando gli elaboratori vengono utilizzati collegati in rete interna non vi è nessuna connessione con l'esterno per cui non esiste il rischio di accesso non autorizzato.	Nessuna durante l'utilizzo.
Ricerche via internet e connessioni a siti per attività della ditta.	Intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale.	Utilizzo di programma "antivirus" aggiornato attivato in modalità "autoprotezione" + scansione antivirus in automatico.
Collegamento alle caselle di posta elettronica per la gestione delle e-mail.	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento	Tenere normalmente scollegato il modem. Limitare il collegamento con modem all'esterno solo ed esclusivamente al tempo necessario alla ditta per attuare le modifiche alle tabelle gestionali o ai programmi. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Verificare periodicamente manualmente che non siano presenti nel sistema programmi "TSR" quali ad esempio "Key Logger'97" oppure "wsock spy" che non vengono identificati dalla protezione antivirus.
Collegamento internet banking.	Violazione e modifica della integrità dei dati con programmi contenenti virus informatici	Utilizzo di programma "antivirus" aggiornato attivato in modalità "autoprotezione" + scansione antivirus in automatico. Limitare il collegamento con modem all'esterno solo ed esclusivamente al tempo necessario ad attuare le modifiche alle tabelle gestionali o ai programmi. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Effettuare controlli periodici a campione per verificare l'integrità

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

Operazioni attuate	Valutazione dei rischi	Misure di protezione e sicurezza
		dei dati archiviati. Effettuare salvataggi periodici dei dati archiviati con conservazione del supporto di back-up in un contenitore in luogo differente da dove è collocato il computer.
Collegamento via internet al sito internet della Società Symantec per effettuare l'aggiornamento del programma antivirus "Norton".	Intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale che eventualmente siano presenti negli strumenti informatici della ditta esterna cui ci si collega per scaricare gli aggiornamenti del programma antivirus.	Utilizzo di programma "antivirus" aggiornato attivato in modalità "autoprotezione" + scansione antivirus in automatico.
	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento.	Limitare il collegamento con modem all'esterno solo ed esclusivamente al tempo necessario per aggiornare il programma antivirus. Non effettuare altri collegamenti alla rete internet al di fuori di quelli autorizzati. Verificare periodicamente manualmente che non siano presenti nel sistema programmi "TSR" quali ad esempio "Key Logger' 97" oppure "wsock spy" che non vengono identificati dalla protezione antivirus.

Postazione nr x: l'elaboratore è utilizzato dal personale di segreteria, responsabile del corretto impiego, che è inoltre stato incaricato del trattamento dei dati personali ed autorizzato all'accesso per la gestione esclusiva delle operazioni connesse alla propria attività lavorativa. E' collegato in rete interna ed esterna mediante server. E' presente Windows XP Professional 2002, programma gestionale, Winzip. Non è possibile caricare programmi o aprire file da supporti esterni quali floppy disk o cd rom.

Operazioni attuate	Valutazione dei rischi	Misure di protezione e sicurezza
Elaborazione testi, tabelle di calcolo, fatturazione clienti. Sono trattati dati personali dei clienti mediante software specifico.	Quando gli elaboratori vengono utilizzati collegati in rete interna non vi è nessuna connessione con l'esterno per cui non esiste il rischio di accesso non autorizzato.	Nessuna durante l'utilizzo.
Ricerche via internet e connessioni a siti per attività della ditta.	Intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale.	Utilizzo di programma "antivirus" aggiornato attivato in modalità "autoprotezione" + scansione antivirus in automatico.
Collegamento alle caselle di posta elettronica per la gestione delle e-mail.	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento	Tenere normalmente scollegato il modem. Limitare il collegamento con modem all'esterno solo ed esclusivamente al tempo necessario alla ditta per attuare le modifiche alle tabelle gestionali o ai programmi. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Verificare periodicamente manualmente che non siano

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

Operazioni attuate	Valutazione dei rischi	Misure di protezione e sicurezza
		presenti nel sistema programmi "TSR" quali ad esempio "Key Logger'97" oppure "wsock spy" che non vengono identificati dalla protezione antivirus.
Collegamento internet banking.	Violazione e modifica della integrità dei dati con programmi contenenti virus informatici	Utilizzo di programma "antivirus" aggiornato attivato in modalità "autoprotezione" + scansione antivirus in automatico. Limitare il collegamento con modem all'esterno solo ed esclusivamente al tempo necessario ad attuare le modifiche alle tabelle gestionali o ai programmi. Non effettuare collegamenti alla rete internet al di fuori di quelli autorizzati. Effettuare controlli periodici a campione per verificare l'integrità dei dati archiviati. Effettuare salvataggi periodici dei dati archiviati con conservazione del supporto di back-up in un contenitore in luogo differente da dove è collocato il computer.
Collegamento via internet al sito internet della Società Symantec per effettuare l'aggiornamento del programma antivirus "Norton".	Intrusione ad opera di programmi di cui all'art. 615-quinquies del codice penale che eventualmente siano presenti negli strumenti informatici della ditta esterna cui ci si collega per scaricare gli aggiornamenti del programma antivirus.	Utilizzo di programma "antivirus" aggiornato attivato in modalità "autoprotezione" + scansione antivirus in automatico.
	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento.	Limitare il collegamento con modem all'esterno solo ed esclusivamente al tempo necessario per aggiornare il programma antivirus. Non effettuare altri collegamenti alla rete internet al di fuori di quelli autorizzati. Verificare periodicamente manualmente che non siano presenti nel sistema programmi "TSR" quali ad esempio "Key Logger' 97" oppure "wsock spy" che non vengono identificati dalla protezione antivirus.

PC nr x: Server, composto di un disco. Serve per il collegamento esterno. Server firewall. Comprende anche sistema autoprotezione dall'esterno

Operazioni attuate	Valutazione dei rischi	Misure di protezione e sicurezza
Collegamento con la rete esterna	Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento.	Tenere normalmente scollegato il modem. Limitare il collegamento con modem all'esterno solo ed esclusivamente al tempo necessario alla ditta per attuare le modifiche alle tabelle

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

Operazioni attuate	Valutazione dei rischi	Misure di protezione e sicurezza
		<p>gestionali o ai programmi. Verificare periodicamente manualmente che non siano presenti nel sistema programmi "TSR" quali ad esempio "Key Logger'97" oppure "wsock spy" che non vengono identificati dalla protezione antivirus.</p>
	<p>Intrusione illecita negli archivi da parte di terzi (pirati informatici) durante il collegamento</p>	<p>Tenere normalmente scollegato il modem. Non effettuare altri collegamenti alla rete internet da questa postazione di lavoro, con esclusione di quello necessario per l'aggiornamento del programma antivirus. Verificare periodicamente manualmente che non siano presenti nel sistema programmi "TSR" quali ad esempio "Key Logger'97" oppure "wsock spy" che non vengono identificati dalla protezione antivirus</p>

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

ANALISI RISCHI E MISURE DI PROTEZIONE E SICUREZZA RELATIVE ALLE AREE E LOCALI

Aree e locali	Valutazione dei rischi	Misure di protezione e sicurezza
Uffici	Intrusione illecita di terzi non autorizzati nei locali dove sono installati i computers.	<p>Gli elaboratori sono installati all'interno dell'ufficio dove possono accedere e sono autorizzati ad essere presenti durante l'orario di lavoro gli incaricati del trattamento dell'ufficio.</p> <p>L'ingresso in questo ufficio da parte di altre persone è autorizzato dagli addetti della segreteria, i quali possono effettuare vigilanza contro il rischio di ingresso di persone non autorizzate.</p> <p>L'accesso agli elaboratori inoltre avviene solo tramite password ed è stata prevista anche la password sullo screen saver che viene attivata automaticamente durante le soste della attività lavorativa.</p> <p>Di giorno, al di fuori dell'orario di lavoro, l'ufficio è chiuso a chiave.</p> <p>Alla sera, al termine dell'orario di lavoro, tutti gli uffici sono chiusi a chiave.</p>
	Incendio-allagamento	<p>Nell'ufficio sono presenti estintori per spegnere eventuali focolai.</p> <p>I dati personali vengono salvati su nastro, e conservati in complete</p> <p>Per il pericolo di allagamento i computers sono in posizione rialzata da terra.</p>
	Mancanza energia elettrica	Presenza di gruppo di continuità per assicurare l'erogazione dell'energia elettrica

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CAPITOLO VII

CRITERI DA ADOTTARE PER LA CIFRATURA E PER LA SEPARAZIONE DI DATI PERSONALI RIGUARDANTI LO STATO DI SALUTE E LA VITA SESSUALE DAGLI ALTRI DATI PERSONALI

DELL'INTERESSATO

7.1. OPERAZIONI EFFETTUATE PER LA CIFRATURA E PER LA SEPARAZIONE DI DATI PERSONALI RIGUARDANTI LO STATO DI SALUTE E LA VITA SESSUALE DELL'INTERESSATO DAGLI ALTRI DATI PERSONALI

I dati cartacei sono raccolti in apposti raccoglitori e archiviati in armadi chiusi mediante serrature/lucchetto a combinazione e utilizzati solo da personale incaricato al trattamento nominati mediante lettera di incarico. I dati trattati informaticamente sono archiviati nel gestionale accessibile solo da personale autorizzato e codificati, completare.

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CAPITOLO VIII

CRITERI DA ADOTTARE E DELLE MODALITA' PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

8.1. OPERAZIONI EFFETTUATE PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

In caso di distruzione/danneggiamento delle apparecchiature hardware è sempre disponibile il supporto rimovibile (nastro magnetico) sul quale vengono effettuati back up giornalieri. Inoltre viene garantita con i fornitori un servizio di assistenza della struttura Hardware e il ripristino dei dati.

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CAPITOLO IX

CRITERI DA ADOTTARE PER GARANTIRE L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTO DI DATI PERSONALI AFFIDATI, IN CONFORMITA' AL CODICE, ALL'ESTERNO DELLA STRUTTURA DEL TITOLARE

9.1 OPERAZIONE EFFETTUATE PER GARANTIRE LE MISURE MINIME DI SICUREZZA IN CASO DI TRATTAMENTO DEI DATI AFFIDATI ALL'ESTERNO

In caso di dati affidati all'esterno, Nome azienda provvede a far sottoscrivere lettera di incarico al trattamento dei dati personali. Gli interessati di questi dati possono essere di :

- soci dell'azienda;
- dipendenti;
- clienti;
- collaboratori;
- fornitori.

Gli incaricati possono essere nei diversi casi:

Soggetti interessati	Tipo di dato					Incaricati esterni del trattamento dei dati
	Personali	Sensibili	Giudiziari	Salute	Vita sessuale	
Soci	X	X	X	X		Commercialista, consulente del lavoro
Dipendenti	X	X		X		Medico, commercialista, collaboratori, consulente del lavoro, azienda manuttrice programmi software.
Collaboratori	X					Azienda manuttrice programmi software, commercialista.
Clienti	X	X		X		Azienda manuttrice programmi software
Fornitori	X					Azienda manuttrice programmi software

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

**CAPITOLO X
PIANO DI FORMAZIONE**

10.1. DEFINIZIONE PIANO DI FORMAZIONE

Annualmente alla fine di un anno commerciale la Direzione della Nome azienda verifica la necessità di promuovere attività formative in materia di:

- informazione sul contenuto e disposizioni del Codice 196/2003.
- definizione dei virus informatici.
- analisi dei rischi derivanti dalla connessione nella rete di telecomunicazioni accessibile al pubblico.
- analisi dei rischi collegati alle aree e locali (intrusione, incendio, ecc.).
- misure pratiche di prevenzione dei rischi.
- misure pratiche per garantire l'integrità dei dati e la sicurezza degli archivi.
- attribuzione delle responsabilità ed autorizzazioni al collegamento in rete esterna.

10.2. SOGGETTI INTERESSATI

Saranno interessati tutti i soggetti individuati con lettera di incarico per i quali sarà organizzato un livello di formazione conforme alla funzione esercitata.

10.3. CONTENUTI, MODALITA' E DOCUMENTAZIONE

Tutti gli incaricati saranno informati dettagliatamente in merito ai contenuti e alle modalità dei corsi, e verrà distribuita appropriata documentazione. La direzione sta già predisponendo l'attuazione o la programmazione di suddetti corsi.

Logo/ragione sociale	DOCUMENTO PROGRAMMATICO SULLA SICUREZZA	Data ultimo aggiornamento:
		Versione 00

CAPITOLO XI

VERIFICA DEL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA

11.1. VERIFICA ANNUALE

Annualmente il responsabile del trattamento dei dati effettua una verifica su:

- documento programmatico per la sicurezza, verificando lo stato di aggiornamento;
- verifica dello stato applicativo delle misure minime di sicurezza stabilite.

L'esito della verifica può portare ad un aggiornamento del DPS e delle misure minime di sicurezza o il mantenimento delle precedenti.

In sede di riunione con la Direzione, il responsabile del trattamento riferisce sullo stato del documento programmatico per la sicurezza e delle misure minime adottate.