VALUTAZIONE DI IMPATTO SULLA PRIVACY DELL'ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI ALESSANDRIA

Regole di comportamento riguardo il trattamento dei dati personali e aziendali, gli strumenti ed i sistemi informatici

Approvato con delibera del Consiglio dell'Ordine in data 05/09/18

CAMPO DI APPLICAZIONE

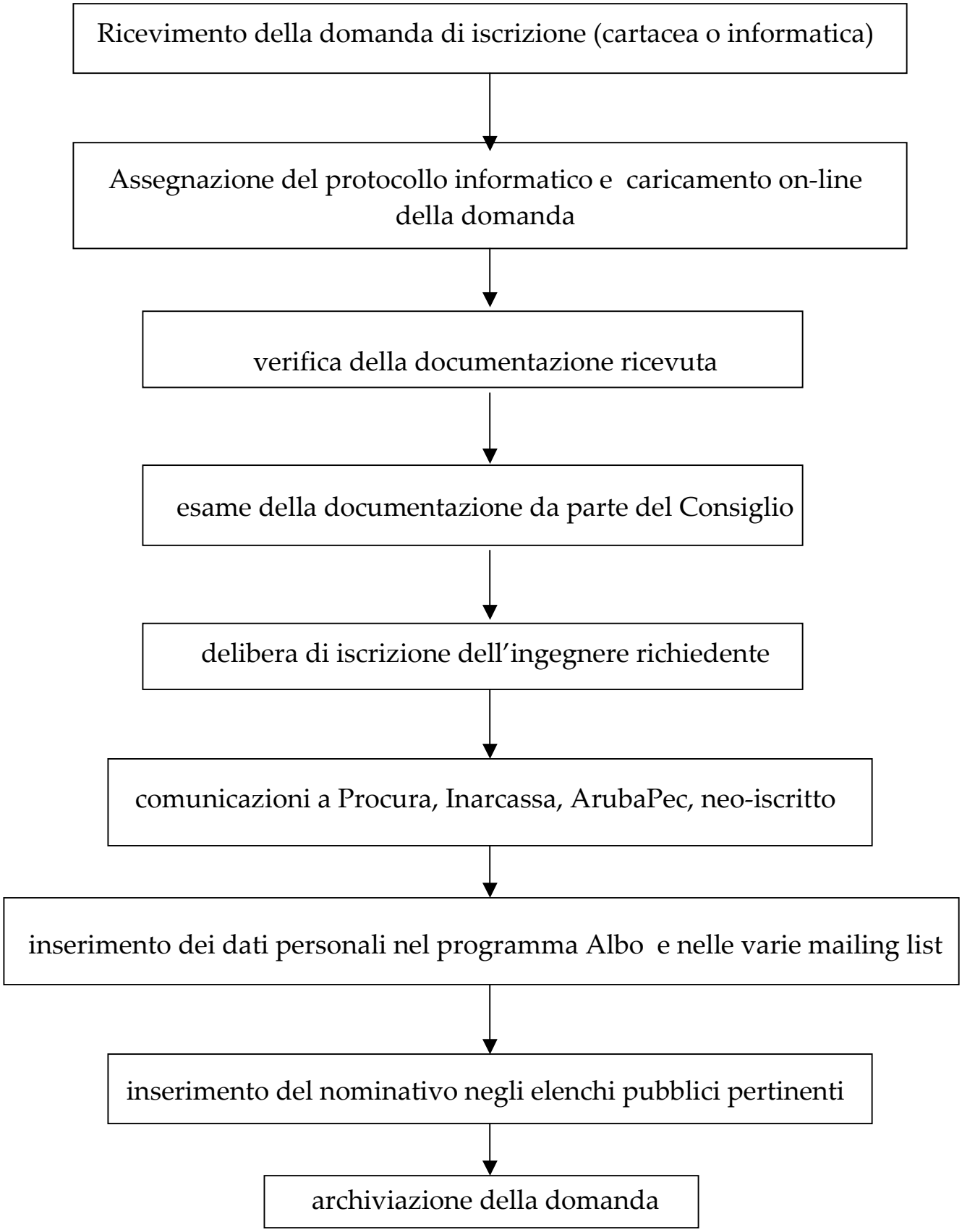
L'Ordine degli ingegneri della provincia di Alessandria è un ente pubblico non economico che ha lo scopo di garantire i cittadini che coloro che sono iscritti nell'Albo sono abilitati ad esercitare la professione di ingegnere e non operano abusivamente.
Per questo motivo vengono trattati dati personali degli iscritti, oltre ai dati personali dei fornitori ed ai dati personali e sensibili dei dipendenti.

ANALISI DEL FLUSSO DEI DATI

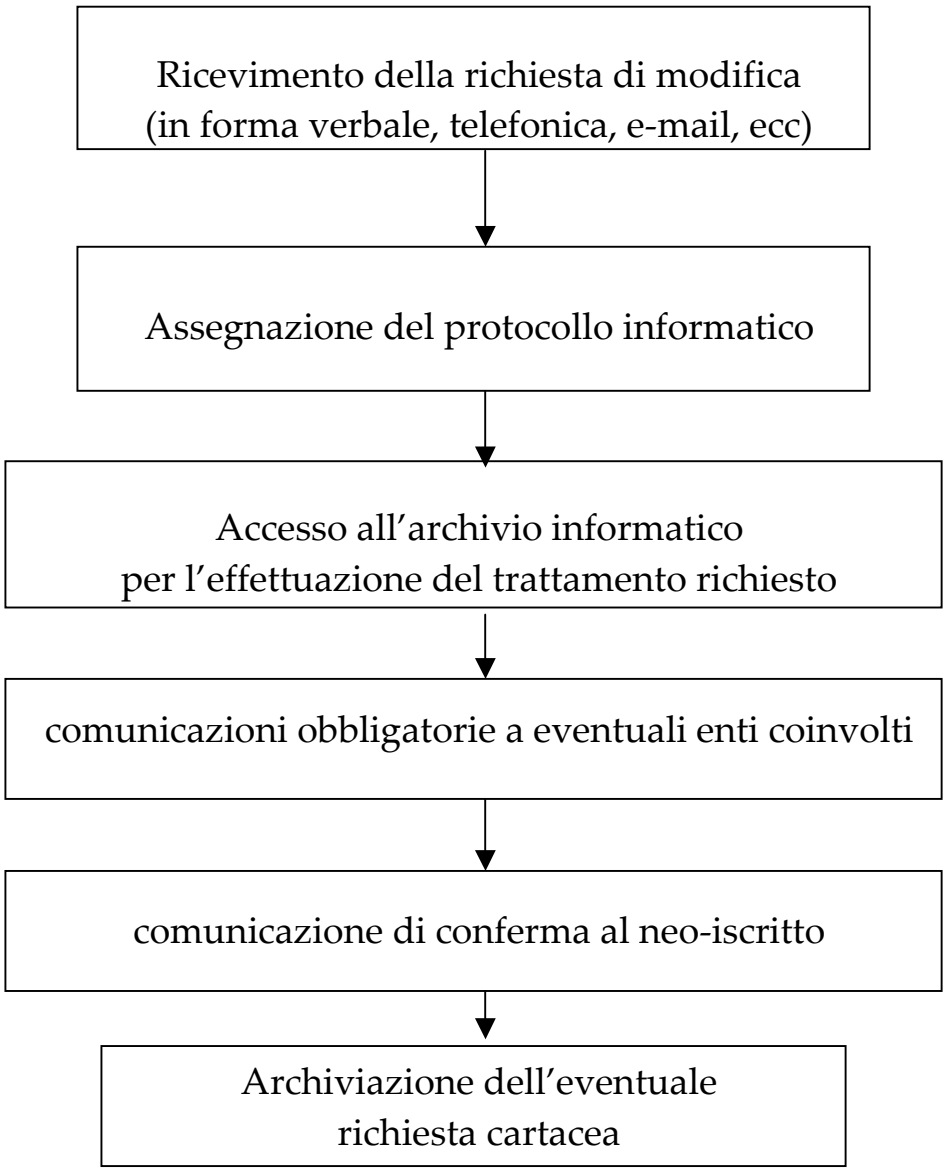
I tipi di trattamento che saranno analizzati sono i seguenti:

- Trattamento dei dati a seguito di iscrizione all'Ordine
- Trattamento a seguito di modifica o integrazione dei dati richiesta dall'iscritto
- Trattamento dei dati dei fornitori
- Trattamento dei dati dei dipendenti tipologia 1
- Trattamento dei dati dei dipendenti tipologia 2

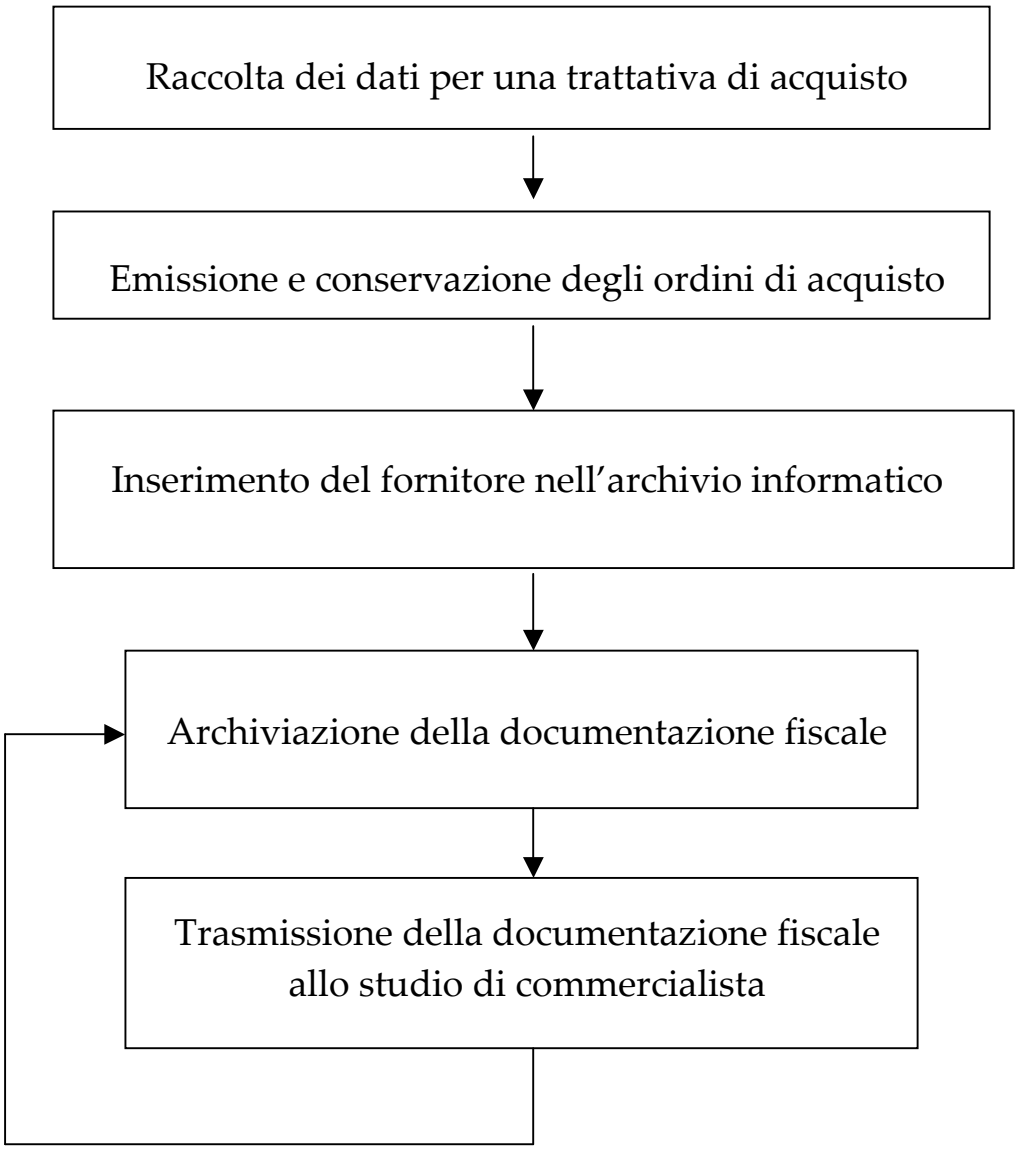
Trattamento dei dati a seguito di iscrizione all'Ordine



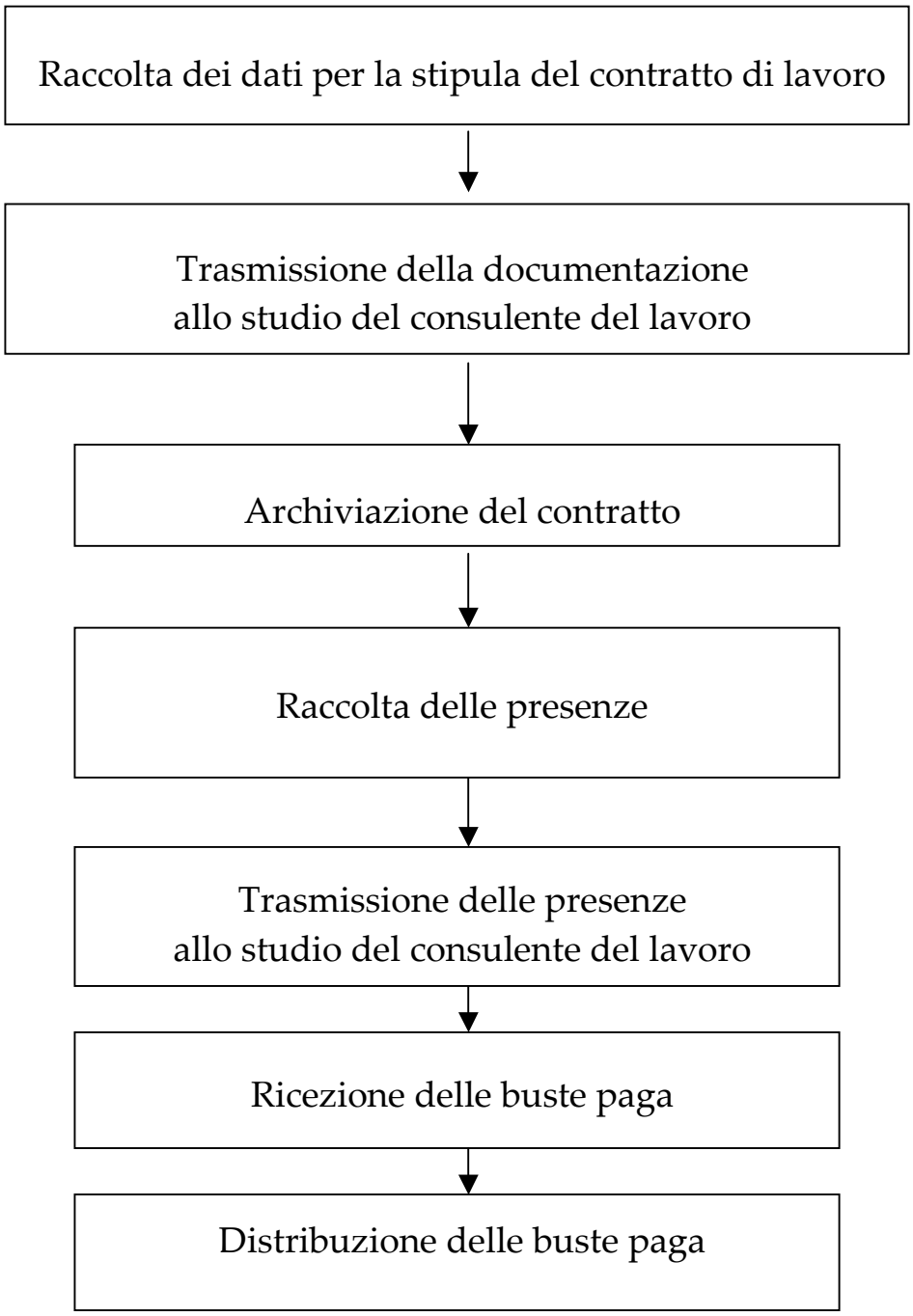
Trattamento a seguito di modifica o integrazione dei dati richiesta dall'iscritto



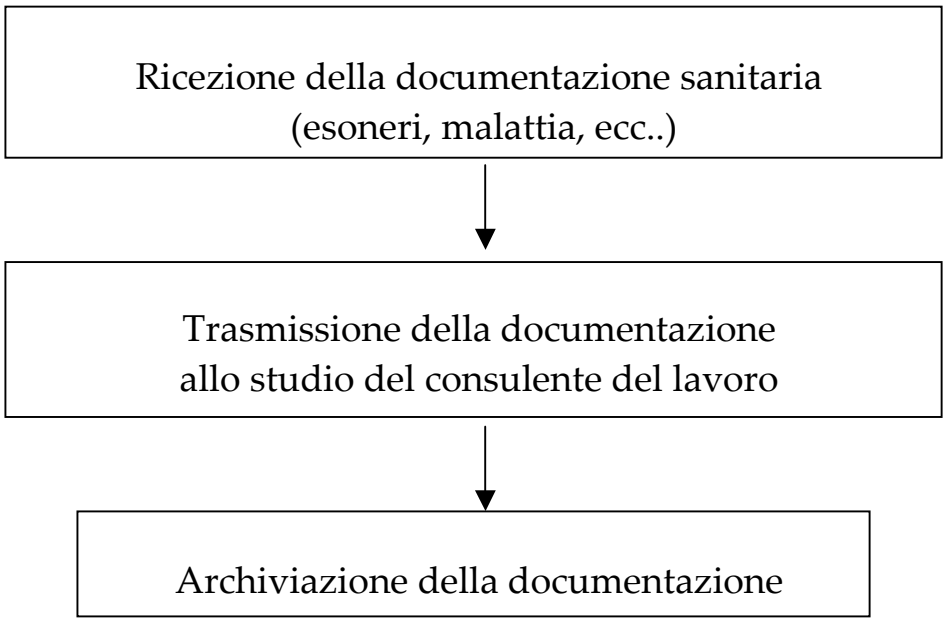
Trattamento dei dati dei fornitori



Trattamento dei dati dei dipendenti tipologia 1



Trattamento dei dati dei dipendenti tipologia 2



VALUTAZIONE DEI RISCHI

Analisi delle possibili situazioni di rischio

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo ed avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare consiste in:

1. individuazione di tutte le risorse del patrimonio informativo;
2. identificazione delle minacce a cui tali risorse sono sottoposte;
3. identificazione delle vulnerabilità
4. definizione delle relative contromisure.

Risorse del patrimonio informativo

I dati personali oggetto di trattamento si trovano in documenti cartacei, documenti elettronici (es. email, tabulati, scansioni) oppure su supporto informatico (database interni ed esterni).
I documenti cartacei (documentazione sugli iscritti, documentazione relativa ad altri enti, fatture attive, passive, buste paga, contratti di lavoro, ordini a fornitori, corrispondenza inviata / ricevuta, ecc..) sono conservati negli armadi predisposti nell'ufficio principale, nell'archivio interno alla sede e nell'archivio posto nel locale cantina, in base alla loro data di emissione.

La tabella seguente riporta l'elenco e la dislocazione dei computer:

Dislocazione	N° apparecchi	Software
Segreteria	2	Applicazioni locali e web
Segreteria	1	Server
Ufficio Presidente	1	Browser internet e software di videoscrittura
Sala corsi	1	Browser internet, software di videoscrittura, software di rilevazione presenze ai corsi, software gestione videocamera
Sala corsi	1	Browser internet e software di videoscrittura e per apertura delle presentazioni

Nella stanza adibita ad archivio è stata installata l'unità di backup da utilizzare in caso di disaster recovery.

Riassumendo i dati precedenti si ottiene la seguente tabella riepilogativa:

Descrizione	Locazione	Tipologia	Supporto	Operatori	Responsabile
Dati iscritti	Segreteria	Personale	Informatico Cartaceo	Baldizzone Cibau	ing. Monica Boccaccio
Dati fornitori	Segreteria	Personale	Informatico Cartaceo	Baldizzone Cibau	ing. Monica Boccaccio
Dati dipendenti	Segreteria	Personale / Sensibile	Informatico Cartaceo	Baldizzone Cibau	ing. Monica Boccaccio
Dati iscritti	Archivio	Personale / Sensibile	Informatico Cartaceo	Baldizzone Cibau	ing. Monica Boccaccio
Dati fornitori	Archivio	Personale	Informatico Cartaceo	Baldizzone Cibau	ing. Monica Boccaccio
Dati dipendenti	Archivio	Personale / Sensibile	Informatico Cartaceo	Baldizzone Cibau	ing. Monica Boccaccio
Dati iscritti	Cantina	Personale	Informatico Cartaceo	Baldizzone Cibau	ing. Monica Boccaccio
Dati fornitori	Cantina	Personale	Informatico Cartaceo	Baldizzone Cibau	ing. Monica Boccaccio
Dati dipendenti	Cantina	Personale / Sensibile	Informatico Cartaceo	Baldizzone Cibau	ing. Monica Boccaccio

Individuazione delle minacce

Le principali minacce da prendere in considerazione riguardano:

- Le risorse hardware
    a. malfunzionamenti dovuti a guasti;
    b. malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
    c. malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica
    d. malfunzionamenti dovuti a sabotaggi e furti.

- Le risorse software
    a. Virus, worms, trojan;
    b. Intercettazioni ed accessi abusivi al sistema;
    c. saturazioni delle risorse disponibili.

- I dati trattati
    a) accesso non autorizzato agli archivi contenenti le informazioni riservate (visione, modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
    b) modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.

- I supporti di memorizzazione
    a) Distruzione e/o alterazione a causa di eventi naturali;
    b) imperizia degli utilizzatori;
    c) sabotaggio;
    d) deterioramento nel tempo (invecchiamento dei supporti);
    e) difetti di costruzione nel supporto di memorizzazione che ne riducono la vita media;
    f) l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

Più dettagliatamente:

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Inondazione	X	X	X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Fuoco	X	X	
Uso di armi		X	
Danno volontario	X		
Interruzione di corrente		X	

Rischi	Deliberato	Accidentale	Ambientale
Interruzione di acqua		X	
Interruzione di aria condizionata	X	X	
Guasto hardware		X	
Linea elettrica instabile		X	X
Temperatura ed umidità eccessive			X
Polvere			X
Radiazioni elettromagnetiche		X	
Scariche elettrostatiche		X	
Furto	X		
Uso non autorizzato dei supporti di memoria	X		
Deterioramento dei supporti di memoria		X	
Errore del personale operativo		X	
Errore di manutenzione		X	
Masquerading dello user-id	X		
Uso illegale di software	X	X	
Software dannoso		X	
Danni sulle linee	X	X	
Intercettazione	X		
Infiltrazione nelle comunicazioni	X		
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X		
Guasto dei sistemi di comunicazione	X	X	
Mancanza di personale		X	
Errore dell'utente	X	X	
Uso non corretto delle risorse	X	X	
Guasto software	X	X	
Uso di software da parte di utenti non autorizzati	X	X	
Uso di software in situazioni non autorizzate	X	X	

Individuazione delle vulnerabilità

Le vulnerabilità del sistema informatico possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nel punto precedente. In particolare le vulnerabilità devono essere ricercate nei seguenti fattori:

- infrastrutture;
- hardware;
- software;
- comunicazioni;
- personale;
- documenti cartacei.

Più dettagliatamente:

Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio (porte, finestre)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autentica-zione
Locazione suscettibile ad allagamenti	Suscettibilità ad umidità, polvere, sporco	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione / invio
	Manutenzione insufficiente	Presenza di linee dial-up con modem
	Carenze di controllo di configurazione (update / upgrade dei sistemi)	Traffico sensibile non protetto
		Connessione a linee pubbliche non protette

Documenti cartacei	Software	Personale
Locali documenti non protetti	Interfaccia uomo – macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione – autenticazione	Mancanza di supervisione degli esterni
Non controllo delle copie	Mancanza dei registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware / software
	Carenza / assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione
	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

Individuazione delle misure protettive

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- contromisure di carattere fisico (ad es. l'adozione di armadi ignifughi in cui conservare documenti cartacei e supporti informatici di backup);
- contromisure di carattere procedurale (ad es. procedure di accesso fisico ai locali, procedure per la gestione delle credenziali di autenticazione);
- contromisure di carattere elettronico / informatico (ad es. l'adozione di un sistema di backup centralizzato, del gruppo di continuità e di un firewall).

Prescrizioni di sicurezza

Il furto o il danneggiamento delle apparecchiature informatiche, la diffusione o distruzione non autorizzata di informazioni personali, anche su formato cartaceo, possono esporre l'Ordine degli ingegneri della provincia di Alessandria al rischio di violare la normativa. Per tale motivo sono istituiti controlli per limitare l'accesso fisico ad alcune aree.

Sono definite aree ad accesso controllato quei locali che contengono apparecchiature informatiche critiche e archivi informatici e/o cartacei contenenti dati personali, per la custodia delle quali viene identificato un "responsabile dell'area".
Il "responsabile dell'area" ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità.
Deve esserci una lista delle persone autorizzate ad accedere.
La lista deve essere periodicamente controllata.
I visitatori occasionali devono essere accompagnati.
Gli ingressi fuori orario devono essere controllati.

Elenco dei responsabili di area

NOME E COGNOME	AREA ASSEGNATA
Bruno Baldizzone	Area 1 Segreteria
Bruno Baldizzone	Area 2 Archivio
Bruno Baldizzone	Area 3 Ufficio Presidente
Bruno Baldizzone	Area 4 Sala corsi
Bruno Baldizzone	Area 5 Cantina

Archivi cartacei

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.

Quando gli atti ed i documenti contenenti dati personali sensibili 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.

Apparecchiature informatiche

Sono considerate apparecchiature informatiche critiche ai fini della sicurezza le seguenti apparecchiature se parte del trattamento di dati personali:

1. computer, sia server che workstation, con la sola esclusione delle workstation ad uso esclusivamente personale;
2. unità a dischi ottici o magnetici e unità nastri (DAT, DLT, ecc.);
3. sistemi per la gestione delle LAN, router, hub, ecc.

Le chiavi dei sistemi e delle apparecchiature devono essere rimosse.

Le apparecchiature delle LAN (Wiring hub, MAU, ecc.) non facenti parte del backbone e non situate nelle aree ad accesso controllate, devono essere riposte almeno all'interno di armadi chiusi.

Sono considerati supporti di memorizzazione i nastri magnetici, le cassette (cartridge), i dischi magnetici o ottici rimovibili, gli hardware removibili, i CD-ROM che contengono informazioni personali.

I supporti devono essere custoditi in un'area ad accesso controllato o in un ufficio che è chiuso quando non presidiato o in un armadio/cassetto chiuso a chiave.

Sono definite informazioni residue quei dati personali ancora leggibili dopo la cessazione di un trattamento. (es. nastri, o dischi magnetici, dischi ottici, ecc.).

I dati personali devono essere resi illeggibili quando non sia più necessario conservarli per gli scopi per cui sono stati raccolti e trattati.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.
La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Sicurezza Logica

Questa sezione disciplina i diversi aspetti del controllo dell'accesso logico alle informazioni personali.
Sono regolamentati gli accessi ai computer alle LAN, alla rete e alle banche dati del sistema informatico.

Funzione Identificazione ed Autenticazione degli utenti: Tale funzione assicura che ad ogni potenziale utente dei sistemi o delle banche dati sia associato un identificativo (user-id). Quando un utente accede al sistema, alla banca dati o alla rete ne viene verificata l'identità mediante un successivo livello di controllo (es. password).

User-id: L'accesso ai sistemi, alle banche dati contenenti informazioni personali, o alla rete deve essere basata sulle effettive necessità del trattamento. L'user-id deve poter essere riconducibile ad un singolo individuo.
L'utilizzo di user-id non personali è normalmente non consentito; potrà essere accettato dal Responsabile del trattamento per casi particolari, ad esempio per applicazioni che permettono la sola lettura delle informazioni.

Assegnazione e revoca delle user-id ed abilitazioni: Il Sig. Bruno Baldizzone, in collaborazione con il tecnico informatico esterno, gestisce la procedura per l'assegnazione delle user-id che permettono l'accesso ai sistemi, alle banche dati ed alla rete dell'Ordine degli ingegneri della provincia di Alessandria
Quando un utente non ha più la necessità di accedere ad una banca dati o lascia l'azienda, il responsabile dell'utente interessato chiederà al Sig. Bruno Baldizzone di disabilitare l'utenza non più necessaria.
Le user-id inutilizzate per più di 6 mesi saranno disattivate.
Non è consentito il riutilizzo di una user-id personale già assegnata ad altro utente.

Password: La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.
Le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione ed al primo utilizzo.
La lunghezza minima della password è di 6 caratteri.
Deve contenere almeno un carattere alfabetico ed uno numerico.
Non deve contenere più di due caratteri identici consecutivi.
Non deve essere simile alla password precedente.
Non deve contenere l'user-id come parte della password.
Deve essere cambiata almeno ogni 6 mesi.
Non deve essere comunicata ad altri utenti.

Dove la tecnologia lo permette tali regole sono rese obbligatorie dal software altrimenti è responsabilità dell'utente rispettarle.

Il ripristino della password deve essere fatta solo a fronte di una positiva identificazione del richiedente e dovrà essere cambiata subito dopo a cura del richiedente.

Programmi pericolosi: I sistemi sensibili ai virus devono essere protetti con opportuni programmi (antivirus). Tali programmi devono essere aggiornati periodicamente.

Connessioni con l'esterno: In un sistema integrato la sicurezza deve essere trattata in modo uniforme, in quanto l'insicurezza di una singola parte si può ripercuotere generando insicurezza in tutto il sistema. Questo vale in particolare per gli aspetti di sicurezza della rete. L'ing. Monica Boccaccio ha il compito di assicurarne la sicurezza nella sua funzione di Responsabile del trattamento.

Per assicurare la sicurezza di una rete è fondamentale controllare gli accessi alla rete stessa. Per questo si danno nel seguito le regole per le connessioni di rete.

Sono considerati connessioni con l'esterno i collegamenti con altre reti, in particolare interconnessioni con i servizi informatici e telematici di altre aziende, incluso Internet.

E' definito Gateway per le interconnessioni esterne l'insieme di hardware, software e applicazioni (es. Firewall o Proxy) che permettono l'interconnessione o l'accesso remoto.
I Gateway devono consentire l'accesso alla rete interna solamente agli utenti autorizzati.
I Gateway di interconnessione esterna sono o sotto il controllo diretto del Sig. Bruno Baldizzone o comunque approvati dall'Ordine degli ingegneri della provincia di Alessandria

L'Ordine degli ingegneri della provincia di Alessandria garantisce che, per la parte di rete/LAN di propria responsabilità e mediante un'opportuna definizione di dominii e/o con l'utilizzo di Firewall, viene evitato il rischio che personale non autorizzato acceda alla rete, ai sistemi o ai dati personali.

SISTEMA DI MONITORAGGIO

Controlli e audit

Il responsabile ICT effettuerà una volta l'anno un test di penetrazione per verificare l'efficacia delle protezioni di sicurezza.
Il Presidente potrà effettuare autonomamente e secondo modalità concordate propri test di penetrazione per verificare l'impossibilità di accedere alla rete se non autorizzati.

I test effettuati a partire dall'esterno della rete dell'Ordine degli ingegneri della provincia di Alessandria cercando di sfruttare eventuali punti di ingresso della rete stessa, potranno essere condotti senza preavviso con frequenza e durata a discrezione del Responsabile ICT che informerà il Presidente e la Segreteria all'inizio ed al termine di ogni test.
I test effettuati dall'interno della rete saranno eseguiti dopo aver dato un preavviso di 7 giorni lavorativi.
Nel caso i test mettano in evidenza delle carenze la situazione deve essere corretta nel più breve tempo possibile.

Accesso remoto e uso dei modem

Le connessioni via modem tra i sistemi e la rete dell'Ordine degli ingegneri della provincia di Alessandria con reti e sistemi esterni possono rappresentare un serio rischio per lo studio stesso. Come conseguenza di collegamenti non corretti dal punto di vista della sicurezza, è possibile che si esponga a rischio l'intero sistema informativo ed i dati in esso contenuti, ciò può avvenire senza che il dipendente se ne renda conto.
Per tale motivo ogni collegamento dall'interno verso l'esterno e viceversa deve rispettare i criteri di sicurezza qui esposti e quelli che verranno stabiliti dal Titolare e/o Responsabile.
Nel caso il collegamento sia di tipo TCP/IP tramite modem, non deve essere permesso il suo uso simultaneamente al collegamento interno.
Di norma i modem collegati alle workstation devono restare spenti se non utilizzati.

Formazione

Il Responsabile del Trattamento ed i Responsabili di area devono essere adeguatamente formati sui contenuti della legislazione vigente, sul percorso logico che ha portato alla redazione di questo documento e sulle loro competenze, nonché sui rischi di non adempimento di tutti i compiti affidati loro.
L'attività di formazione sarà svolta, compatibilmente con le esigenze di lavoro, dal Responsabile dello studio che ha predisposto questo documento.

MISURE CORRETTIVE

Le piattaforme contenenti i dati personali dei clienti sono esterne all'azienda, pertanto sono state acquisite copie delle impostazioni di tutela della sicurezza dei dati e delle varie misure predisposte.
Il responsabile ICT provvede a mantenere antivirus, antispyware e antimalware aggiornati, in modo da verificare e monitorare eventuali accessi non autorizzati.
Il personale è stato adeguatamente formato e informato e periodicamente il responsabile provvede ad effettuare audit di monitoraggio sulle operazioni di trattamento effettuate in azienda.
In caso di incidente, visto che i dati personali raccolti non mettono a rischio i diritti e le libertà degli individui (danno reputazionale, perdite finanziarie..), si provvederà ad una comunicazione pubblica per informare i soggetti interessati.

PIANI DI RIPRISTINO DELLA NORMALE OPERATIVITA'

La procedura di disaster recovery si basa sull'utilizzo di un server interno su cui vengono copiati giornalmente i dati dell'applicativo on line, garantendo una ridondanza logico/fisica delle informazioni; l'azienda mantiene in background il precedente sistema gestionale che può essere riattivato in caso di problemi dell'applicativo on line.