INDICE

Rev	Data	Descrizione	Verificato	Approvato
0	09.07.2018	Prima Emissione	O.d.V.	C.d.A. Assemblea soci

1. SCOPO

La presente procedura ha lo scopo di assicurare la qualità dei servizi informatici e di telecomunicazioni all'interno dell'azienda, al fine di garantire il buon funzionamento dei servizi correlati e la prevenzione della frode informatica di cui al modello organizzativo.

2. GENERALITA'

- Modello Organizzativo – Parte speciale A

3. CAMPO DI APPLICAZIONE

Si applica a tutte le attività di sviluppo e gestione della rete informatica aziendale e delle apparecchiature di telecomunicazioni.

4. RESPONSABILI

La responsabilità della gestione della rete Informatica e della flotta degli apparati informatici è dell'Amministratore di Rete.

La responsabilità della sicurezza e della riservatezza generale del Sistema Informatico è del Direttore Amministrativo.

5. REGOLE

5.1.1 Acquisto di nuove apparecchiature hardware e/o software di base

In connessione con lo sviluppo di nuove applicazioni software, e/o con la installazione di nuovi pacchetti applicativi, può essere necessario acquisire nuovi componenti hardware e/o software di base.

Tale esame, che si concretizza in un'accurata ricerca di mercato, viene generalmente condotto dall'Amministratore di rete congiuntamente ai settori aziendali interessati.

L'individuazione di un prodotto idoneo dà luogo ad una richiesta di acquisto del pacchetto e di fornitura di servizi e/o prodotti collaterali (installazione, personalizzazione, addestramento, training etc).

La procedura di acquisizione si conclude con un collaudo che viene espresso sulla fattura finale di pagamento al fornitore, salvo il caso in cui non sia esplicitamente previsto un verbale di collaudo.

L'acquisto di nuovo hardware e/o software di base può nascere anche dalla necessità di eliminare le obsolescenze o di ampliare l'utenza.

5.1.2 Fornitura di risorse hardware e/o software nuove o sostitutive di quelle già in dotazione

La necessità di acquisire nuove risorse hardware e/o software di base può insorgere o in esito allo sviluppo di piani operativi, o per incremento del numero

di utenti, o per fisiologiche necessità di adeguamenti tecnologici evolutivi. In seguito ad approvazione della proposta si procede all'acquisto.

5.1.3 Gestione sicurezza informatica

Le piattaforme di gestione e controllo impiegate sono viste come server di applicazioni.

La politica di sicurezza sulla rete è garantita da una politica di backup giornaliera ed automatica.

L'accesso ai server è protetto sia dal punto di vista fisico, sia dal punto di vista della sicurezza informatica (controllo degli accessi dall'esterno, password per gli accessi dall'interno, antivirus aggiornati).

L'Amministratore di rete gestisce l'elenco dei posti di lavoro con le relative configurazioni hardware e software e password, la cui documentazione è conservata in luogo protetto.

5.1.4 Gestione Sicurezza e Riservatezza dati

Per sicurezza dei dati si intende di seguito la protezione dei dati su supporto informatico tese a garantire la loro integrità e/o ricostruibilità rispetto a danneggiamenti derivanti da una qualsivoglia causa esterna, nonché la protezione del sistema informatico aziendale rispetto a guasti o malfunzionamenti di varia natura tendenti a ridurre i tempi di interruzione del servizio dal sistema stesso erogato.

La politica di sicurezza della rete è garantita, inoltre, da un sistema di Firewall che impedisce intrusioni indesiderate di utenti dall'esterno della rete e da un sistema di antivirus che blocca i virus conosciuti all'atto in cui essi tentano di installarsi sul sistema, in dotazione anche ai PC utenti.

Gestione Riservatezza

Per riservatezza si intende di seguito la protezione dei dati da accessi impropri o fraudolenti.

La politica di riservatezza della rete è garantita da:

a) In generale:

- Una selettiva politica di accesso alle banche dati della Pubblica Amministrazione, fiscali e previdenziali, finalizzate ad impedire alterazioni dei dati fiscali dopo la comunicazione. I dipendenti autorizzati a tale accesso sono ben individuati, accedono alle comunicazioni telematiche attraverso specifiche password, trasmettono file che vanno in accodamento a quelli trasmessi in precedenza. Le trasmissioni non sono interattive, ma di tipo batch, per cui si risale con certezza all'autore delle singole trasmissioni.
- Una politica tendente ad impedire un inserimento improprio di dati su bonifici di pagamento e dati contabili. Tale politica è perseguita

attraverso un accesso ai dati contabili protetti da password; le trasmissioni telematiche delle disposizioni di pagamento alle banche vengono effettuate tramite dispositivi specifici protetti da password di accesso alle varie fasi procedurali; vengono effettuati, infine, controlli di quadratura sui resoconti bancari.

- Una politica di adozione del SW applicativo tendente ad eliminare il rischio di sviluppo di software che permetta la commissione di reati. Ciò viene ottenuto attraverso l'adozione e l'uso di pacchetti standard presenti sul mercato; eventuali personalizzazioni vengono richieste al fornitore per iscritto e controllate e collaudate dall'organismo aziendale richiedente.
- Una politica di adozione del software applicativo tendente ad eliminare errori che possono provocare reati tipo la truffa (consapevoli o inconsapevoli). Ciò viene ottenuto attraverso le procedure descritte al punto precedente e ricorrenti controlli sui risultati delle elaborazioni, in particolare per le procedure contabili e le procedure "paghe".
- Una politica tendente ad impedire alterazione dei dati contabili presenti sul sistema, attraverso un accesso controllato ai dati, protetto da password.