1. GESTIONE RETE INFORMATICA

1.1 SCOPO

La presente procedura definisce le azioni e le modalità di gestione della rete informatica (Hardware e Software) dell'Azienda.

1.2 CAMPO DI APPLICAZIONE

La procedura riguarda le attività di:

A) MANUTENZIONE HW E MACCHINE ELETTRONICHE

B) ARCHIVIAZIONE STATO PATRIMONIO

C) ANTIVIRUS

D) BACK-UP ARCHIVI CONDIVISI
Preservazione e salvaguardia dei dati e delle procedure informatiche per garantire l'integrità degli stessi, attraverso back-up differenziati e verifiche periodiche degli stessi (disaster recovery plan)

E) VIOLAZIONE DATI PERSONALI (DATA BREACH)
Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, da divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati

1.3 RESPONSABILITÀ

La responsabilità della gestione del sistema informatico dell'addetto all'Ufficio sviluppo informatico e per alcuni aspetti direttamente del Titolare del Trattamento
La responsabilità dell'aggiunta di nuovo HW/SW e/o implementazione di quello esistente è dei dirigenti di area.

1.4 ALLEGATI

- Schede PC e periferiche connesse (informatiche)
- Documento Programmatico sulla Sicurezza
- Regolamento utilizzo Sistema Informativo
- PG 01 - A : Scadenziario Disater-Recovery
- PG 01 – B : Registro delle violazioni

Il Direttore
dott. Alberto Pinto

_____

	PTPC	**D.Lgs 231/01**
Area / ambito del rischio	Area provvedimenti ampliativi della sfera giuridica dei destinatati- utilizzo delle rete per finalità non istituzionali, strumentali alla realizzazione di eventi corruttivi	pirateria informatica o utilizzo delle rete per finalità non istituzionali

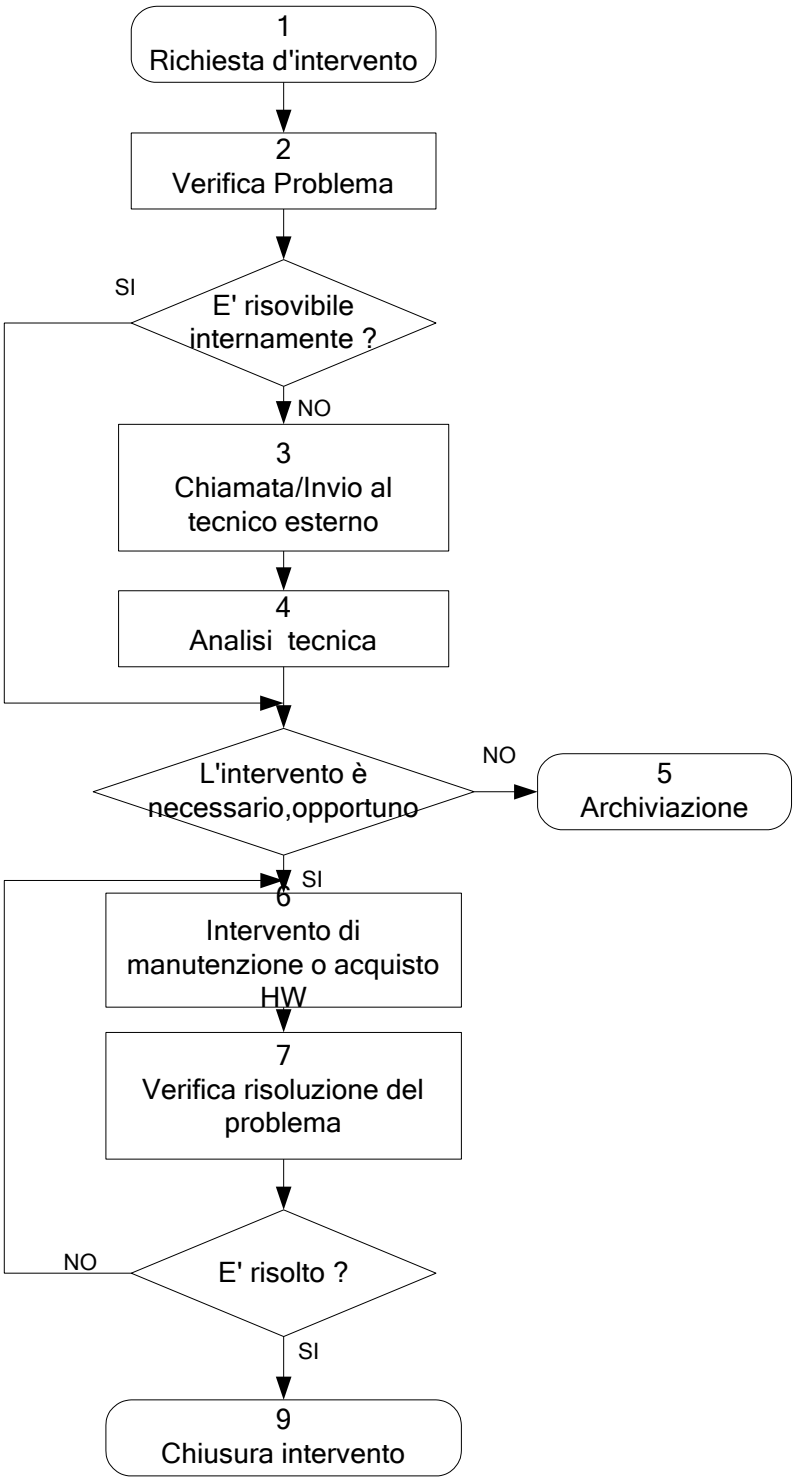
Frequenza	Rilevanza esterna	Precedenti accadimenti	Poteri e strumenti	Discrezionalità	PROBABILITA’
0,6	0,4	0,0	0,8	0,2	2,0 = Bassa

PROBABILITA’	Bassa	IMPATTO	Alto	Liv. di RISCHIO	BASSO

Deleghe e procure	Misure org.ve	Segregazione compiti	Tracciabilità	Sistema di controllo	LIVELLO DI CONTROLLO
	1		1	1	3,0 = Medio

Azioni finalizzate alla riduzione del livello di rischio e documenti di riferimento	PTPC/ D. Lgs 231	Sic.Lav. 8108	Privacy e Sicurezza
- firewal e antivirus aggiornati - i singoli utenti sono abilitati solo per le attività da svolgere - solo l’Amministratore di sistema ha le abilitazioni necessarie - Codice Etico Aziendale. - Regolamento sull'utilizzo del Sistema Informatico. - Procedura per eventuali casi di "Data Breach".	X		
Fase/Elementi da verificare in Audit	**PTPC/ D. Lgs 231**	**Sic.Lav. 8108**	**Privacy e Sicurezza**
- aggiornamento firewall e antivirus - accessi non autorizzati a campione	X		

A – Manutenzione HW e macchine elettroniche



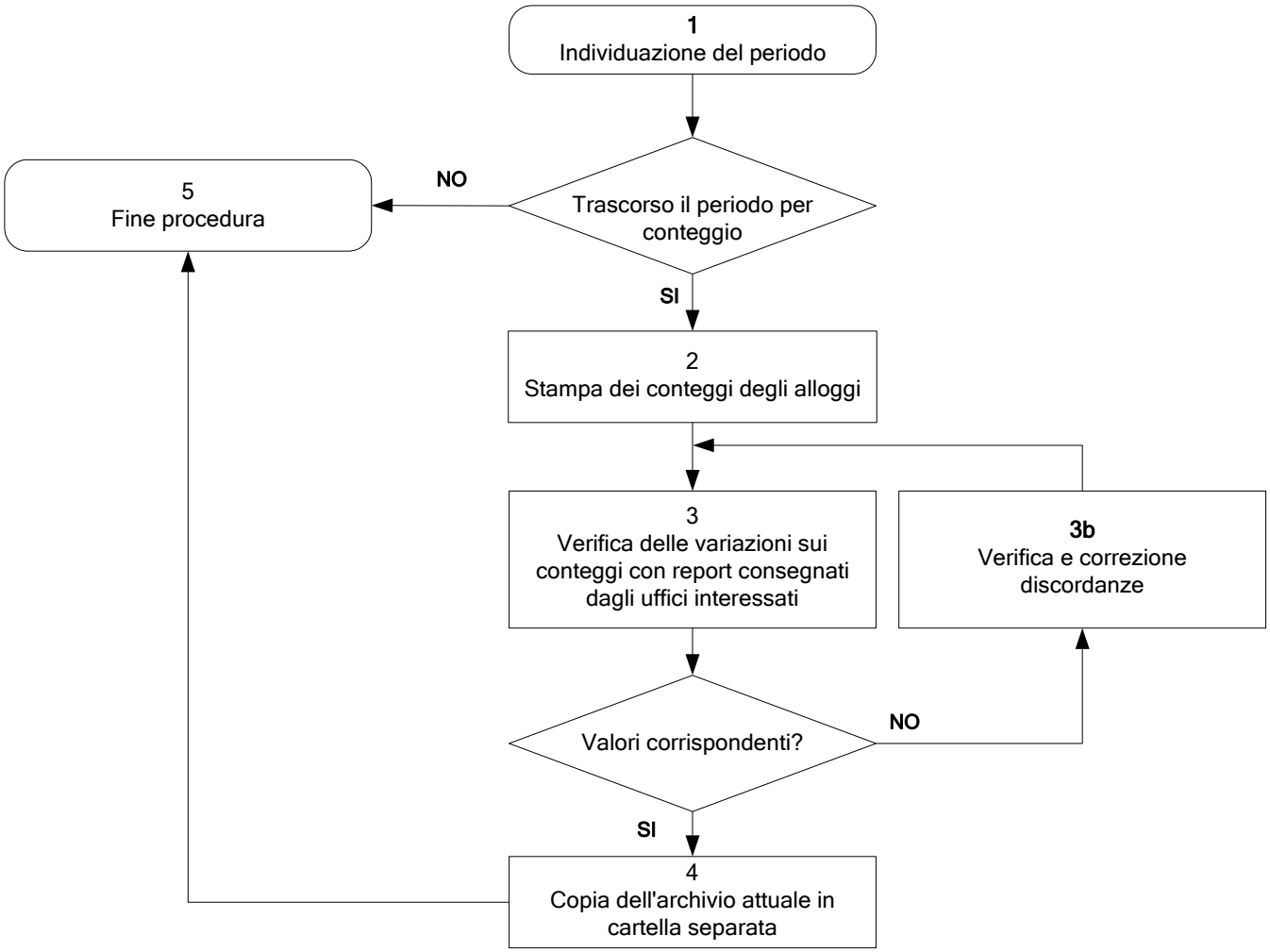
Settore: Informatica	Processo: A - Manutenzione HW e macchine elettroniche	Responsabile: Resp. sviluppo informatico

N	Attività	Responsabile attività	Risorse umane	Attrezzatura mezzi e supporti	Materiali documenti da elaborare	Know-how norme-regole da rispettare	Prodotti	Cliente o destinatario	Parametro/ indicatore
1	Richiesta di intervento	Responsabile dell'ufficio	Addetto dell'ufficio	Comunicazione				Responsabile sviluppo informatico	1 ora
2	Verifica del problema	Dirigente di area	Responsabile sviluppo informatico	HW e SW	Analisi del guasto	conoscenza HW e SW	**esito verifica**	Responsabile sviluppo informatico	1-2 ore
3	Chiamata/Invio al tecnico esterno	Dirigente di area	Responsabile sviluppo informatico	Comunicazione telefonica, scritta		conoscenza HW e SW	**definizione eventuale intervento esterno**	Responsabile sviluppo informatico	In giornata
4	Analisi tecnica	Dirigente di area	Tecnico esterno				**esito analisi**	Responsabile sviluppo informatico	In giornata
5	Archiviazione								1 ora
6	Intervento di manutenzione o acquisto HW	Dirigente di area	Responsabile sviluppo informatico; Tecnico esterno	HW e SW		conoscenza HW e SW	**Soluzione del problema**		in settimana
7	Verifica soluzione del problema	Dirigente di area	Responsabile sviluppo informatico	HW e SW		conoscenza HW e SW	**esito verifica**	Responsabile sviluppo informatico	1-2 ore

Settore: Informatica	Processo: A - Manutenzione HW e macchine elettroniche	Responsabile: Resp. sviluppo informatico

N	Attività	Responsabile attività	Risorse umane	Attrezzatura mezzi e supporti	Materiali documenti da elaborare	Know-how norme-regole da rispettare	Prodotti	Cliente o destinatario	Parametro/ indicatore
8	Chiusura intervento	Dirigente di area	Responsabile sviluppo informatico				**esito positivo verifica**		

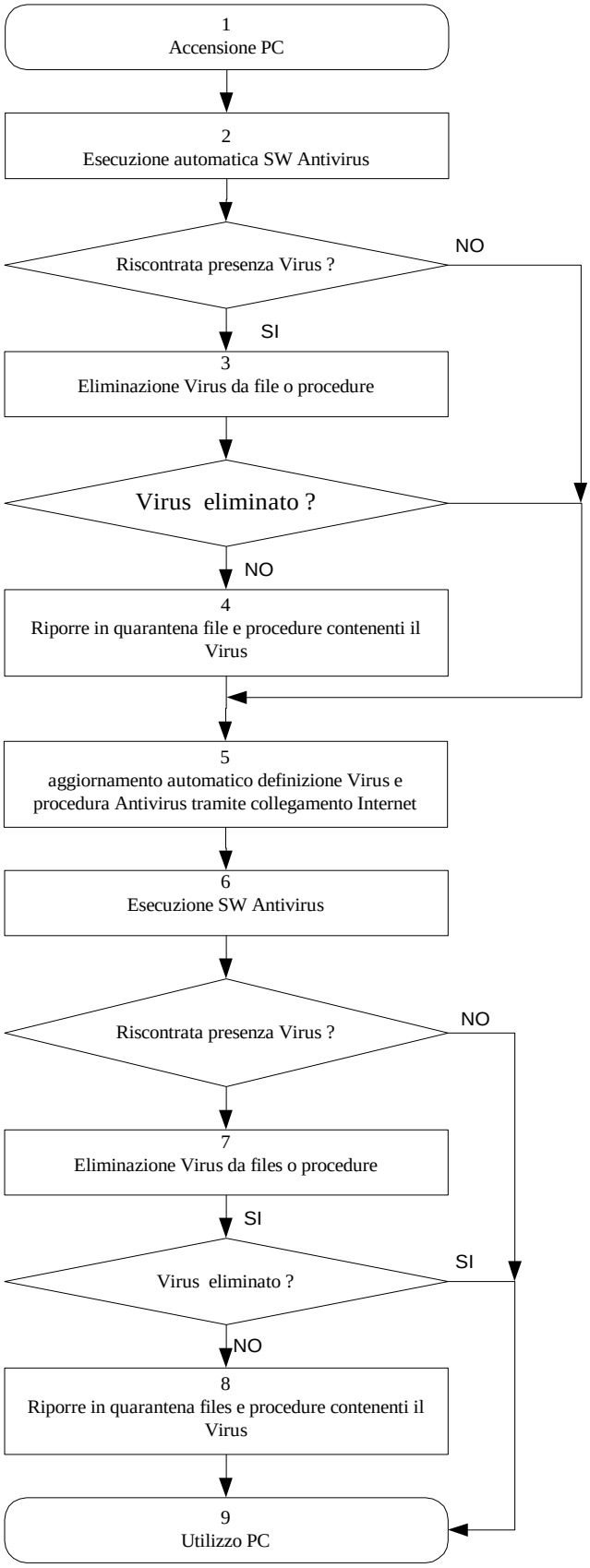
B - Archiviazione stato patrimonio



Settore: Patrimonio/Inquilinato	Processo: B - Archiviazione stato patrimonio	Responsabile: Resp. sviluppo informatico

N	Attività	Responsabile attività	Risorse umane	Attrezzatura mezzi e supporti	Materiali documenti da elaborare	Know-how norme-regole da rispettare	Prodotti	Cliente o destinatario	Parametro/ indicatore
1	Individuazione del periodo	Dirigente area Amministrativa	Responsabile sviluppo informatico.						giornalmente
2	Stampa dei conteggi degli alloggi	Dirigente area Amministrativa	Responsabile sviluppo informatico.	SW Gestione Inquilini			Stampa conteggi alloggi	Responsabile sviluppo informatico.	ogni 15 giorni
3	Verifica delle variazioni sui conteggi con report consegnati dagli uffici interessati	Dirigente area Amministrativa	Dipendenti uffici Inquilinato; Patrimonio; Vendite e CED	HW e SW appr.	Rapportino		Registrazione	Responsabile sviluppo informatico.	ogni 15 giorni
3b	Verifica e correzione discordanze	Dirigente area Amministrativa	Dipendenti uffici Inquilinato; Patrimonio; Vendite e CED	HW e SW appr.					ogni 15 giorni se necessario
4	Copia dell'archivio attuale in cartella separata	Dirigente area Amministrativa	Responsabile sviluppo informatico.	HW e SW appr.			Copia archivi	Sistema Informativo	ogni 15 giorni
5	Fine procedura	Dirigente area Amministrativa	Responsabile sviluppo informatico.	HW e SW appr.			Archiviazione documenti	Responsabile sviluppo informatico.	Giornalmente

C – ANTIVIRUS


1
Accensione PC
2
Esecuzione automatica SW Antivirus
Riscontrata presenza Virus ?
NO
SI
3
Eliminazione Virus da file o procedure
Virus eliminato ?
NO
4
Riporre in quarantena file e procedure contenenti il Virus
5
aggiornamento automatico definizione Virus e procedura Antivirus tramite collegamento Internet
6
Esecuzione SW Antivirus
Riscontrata presenza Virus ?
NO
7
Eliminazione Virus da files o procedure
SI
Virus eliminato ?
SI
NO
8
Riporre in quarantena files e procedure contenenti il Virus
9
Utilizzo PC

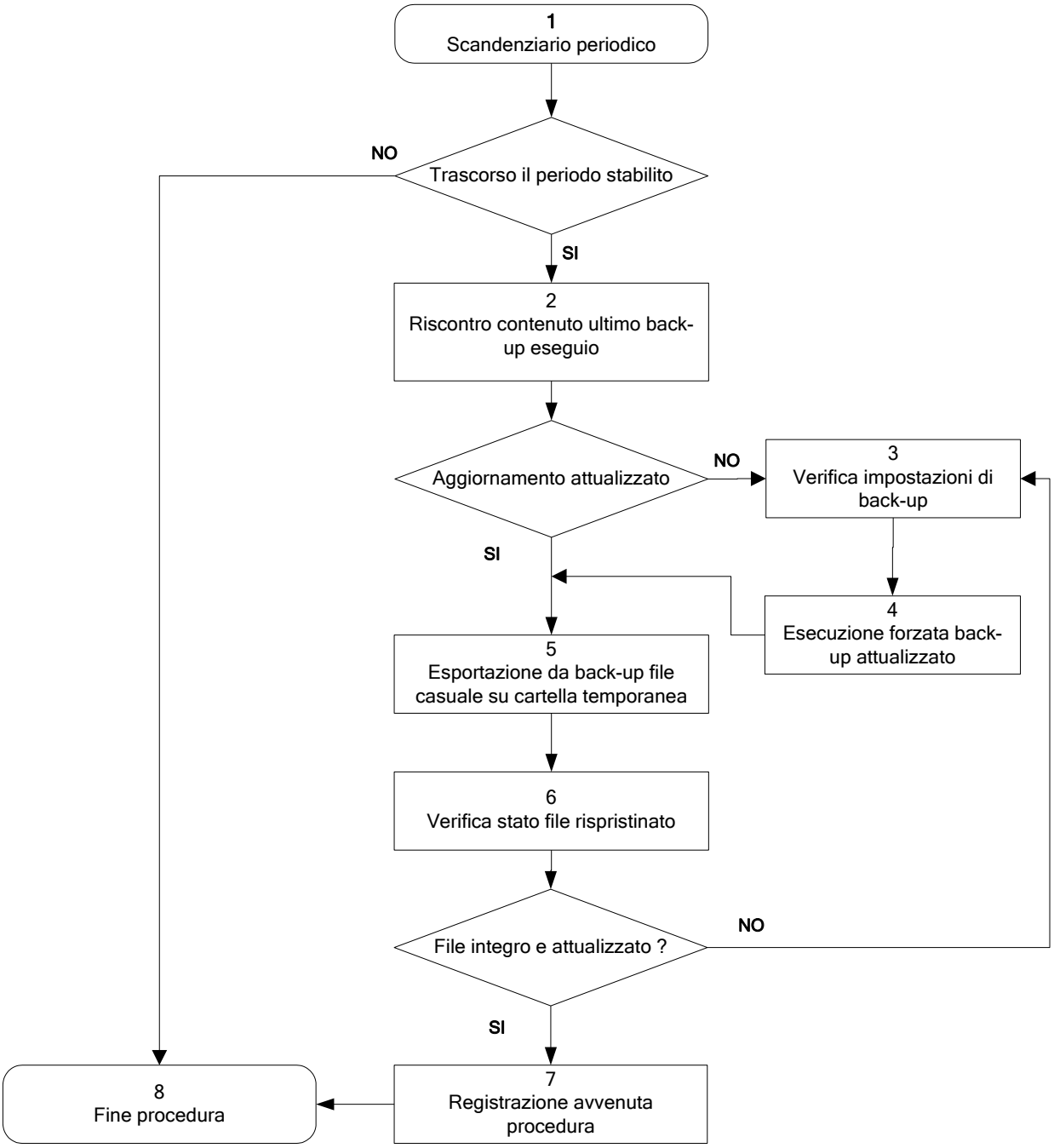
Settore: Informatico	**Processo: C - Antivirus**	**Responsabile: Resp. sviluppo informatico**

N	Attività	**Responsabile attività**	**Risorse umane**	**Attrezzatura mezzi e supporti**	**Materiali documenti da elaborare**	**Know-how norme-regole da rispettare**	**Prodotti**	**Cliente o destinatario**	**Parametro/ indicatore**
1	Accensione PC	Addetto PC	Addetto PC	PC e SW Antivirus		Piano Sicurezza Archivi		Sistema Informativo	-
2	Esecuzione automatica SW Antivirus	Addetto PC	Addetto PC.	PC e SW Antivirus		Piano Sicurezza Archivi i		Sistema Informativo	1 ora
3	Eliminazione Virus da File e Procedure			PC e SW Antivirus		Piano Sicurezza Archivi		Sistema Informativo	1-2 ore
4	Riporre in quarantena File e Procedure contenenti Virus			PC e SW Antivirus		Piano Sicurezza Archivi	file e procedure in quarantena	Sistema Informativo	-
5	Aggiornamento automatico definizioni Virus e procedura Antivirus tramite collegamento a Internet	Dirigente di area	Responsabile sviluppo informatico.	PC e SW Antivirus		Piano Sicurezza Archivi		Sistema Informativo	Aggiornamento ogni 2 settimanale
6	Esecuzione SW Antivirus	Addetto PC	Addetto PC.	PC e SW Antivirus		Piano Sicurezza Archivi		Sistema Informativo	-
7	Eliminazione Virus da file e procedure			PC e SW Antivirus		Piano Sicurezza Archivi		Sistema Informativo	1-2 ore

Settore: Informatico	**Processo: C - Antivirus**	**Responsabile: Resp. sviluppo informatico**

N	Attività	**Responsabile attività**	**Risorse umane**	**Attrezzatura mezzi e supporti**	**Materiali documenti da elaborare**	**Know-how norme-regole da rispettare**	**Prodotti**	**Cliente o destinatario**	**Parametro/ indicatore**
8	Riporre in quarantena file e procedure contenenti Virus			PC e SW Antivirus		Piano Sicurezza Archivi	file e procedure in quarantena	Sistema Informativo	-
9	Utilizza PC	Addetto PC	Addetto PC.	PC e SW Antivirus		Piano Sicurezza Archivi	file e procedure in quarantena	Sistema Informativo	in giornata

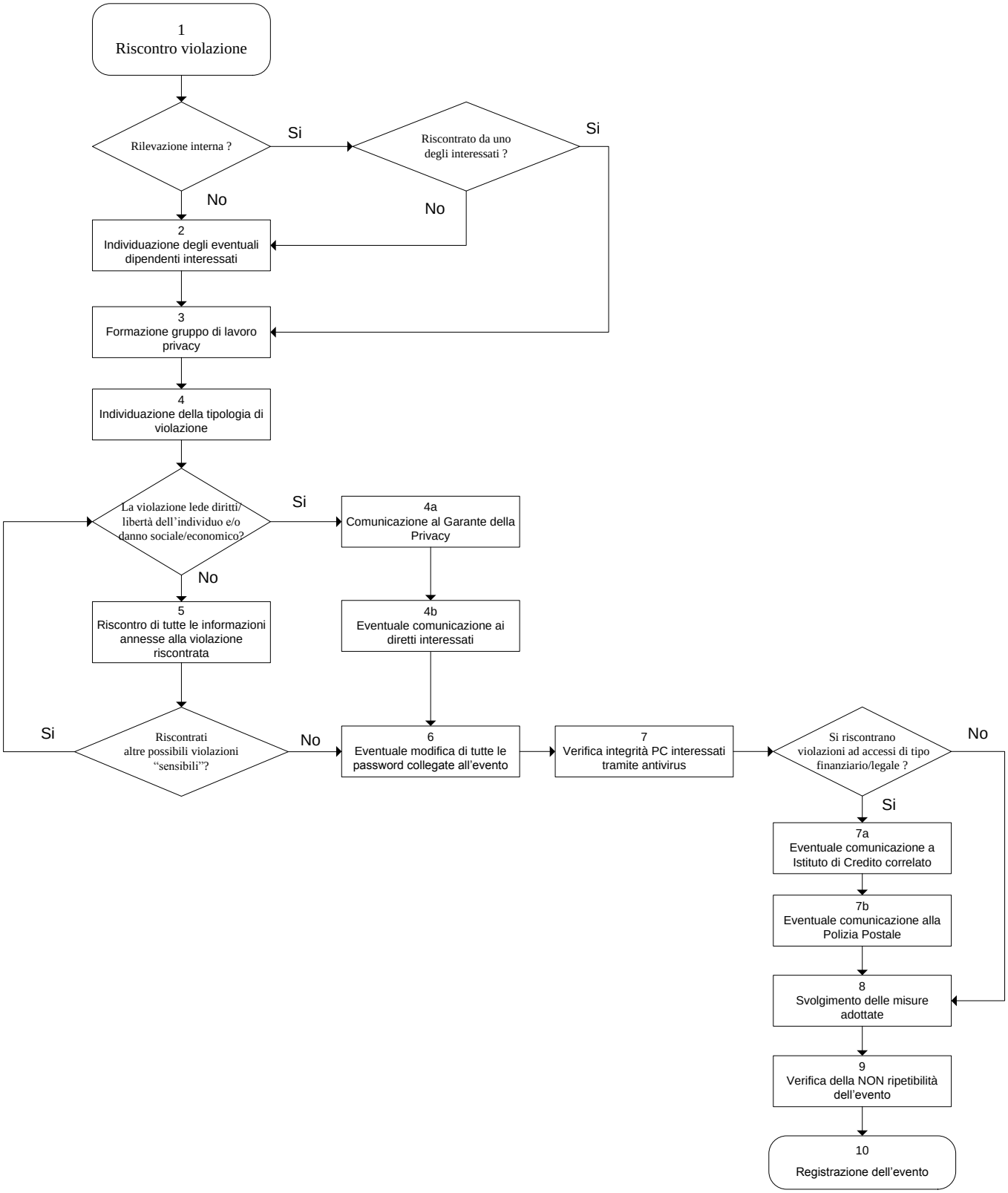
D – Disaster Recovery



Settore: Informatico	**Processo: D – Disaster Recovery**	**Responsabile: Resp. sviluppo informatico**

N	Attività	**Responsabile attività**	**Risorse umane**	**Attrezzatura mezzi e supporti**	**Materiali documenti da elaborare**	**Know-how norme-regole da rispettare**	**Prodotti**	**Cliente o destinatario**	**Parametro/ indicatore**
1	Scadenziario periodico	Responsabile CED	Responsabile CED	Server & NAS		Tempistiche scadenziario	Aggiornamento scadenziario		2 volte l'anno
2	Riscontro contenuto ultimo bck-up eseguito	Responsabile CED	Responsabile CED	Server & NAS			comparazione contenuto file con vigente (esistente)		in giornata
3	Verifica impostazioni di back-up	Responsabile CED	Responsabile CED	Software di back-up e/o operazioni pianificate su Server			Eventuale aggiornamento valori		in giornata
4	Esecuzione forzata back-up attualizzato	Responsabile CED	Responsabile CED	Server & NAS + Software back-up	Nuovi file/cartelle back-up dello stato attuale del sistema		Nuovo back-up		in giornata
5	Esportazione da back-up file casuale su cartella temporanea	Responsabile CED	Responsabile CED	Server & NAS + Software back-up			File casuale da back-up		in giornata
6	Verifica stato file ripristinato	Responsabile CED	Responsabile CED	Server & NAS			Verifica file da bck-up con esistente		in giornata
7	Registrazione avvenuta procedura	Responsabile CED	Responsabile CED		Scadenziario Desater-Recovery (PG 01-A)	\	Registrazione evento		in giornata
8	Fine procedura	Responsabile CED	Responsabile CED		Scadenziario Desater-Recovery (PG 01-A)				in giornata

E – Data Breach



Settore: Privacy/Informatico	**Processo: E – Data Breach**	**Responsabile: Titolare del Trattamento**

N	Attività	**Responsabile attività**	**Risorse umane**	**Attrezzatura mezzi e supporti**	**Materiali documenti da elaborare**	**Know-how norme-regole da rispettare**	**Prodotti**	**Cliente o destinatario**	**Parametro/ indicatore**
1	Riscontro violazione					Regolamento UE 2016/679; D.Lgs. 101/2018	Segnalazione anomalia/infrazione		
2	Individuazione degli eventuali dipendenti interessati		Responsabile CED	Software/attrezzatura correlata/Privacy	Segnalazione evento all'ufficio/area interessata	art.29 Linee Guida delle Violazioni	Comunicazione immediata		entro 12 ore
3	Formazione gruppo di lavoro privacy	Titolare del trattamento							
4	Individuazione della tipologia di violazione	Responsabile d'ufficio (1); Responsabile CED (2) ; Dirigente	Responsabile d'ufficio (1); Responsabile CED (2) ; Dirigente		Segnalazione al DPO	Regolamento UE 2016/679; D.Lgs. 101/2018	Verbalizzazione evento		entro 12 ore
4a	Comunicazione al Garante della Privacy	Dirigente		PEC/ Raccomandata	Apposito modulo da sito garante		Segnalazione ala Garante della Privacy	Garante Privacy	Entro 72 ore dal riscontro dell'evento
4b	Eventuale comunicazione ai diretti interessati	Responsabile d'ufficio (1); Responsabile CED (2) ; Dirigente					Segnalazione ai diretti interessati		
5	Riscontro di tutte le informazioni annesse alla violazione	Responsabile d'ufficio (1); Responsabile CED (2) ; Dirigente				Regolamento UE 2016/679; D.Lgs. 101/2018			
6	Eventuale modifica di tutte le password collegate all'evento	Amministratore di Sistema	Responsabile CED	Software correlati			Reset sistema sicurezza PC/Rete	Rete/PC aziendali	Nel più breve tempo possibile

Settore: Privacy/Informatico	**Processo: E – Data Breach**	**Responsabile: Titolare del Trattamento**

N	Attività	**Responsabile attività**	**Risorse umane**	**Attrezzatura mezzi e supporti**	**Materiali documenti da elaborare**	**Know-how norme-regole da rispettare**	**Prodotti**	**Cliente o destinatario**	**Parametro/ indicatore**
7	Verifica integrità PC interessati tramite antivirus	Amministratore di Sistema	Responsabile CED	Software correlati			Reset sistema sicurezza PC/Rete	Rete/PC aziendali	Nel più breve tempo possibile
7a	Eventuale comunicazione a Istituto di Credito correlato	Ufficio Ragioneria		Protocollo	Protocollo in partenza		Segnalazione a Istituto di Credito	Istituto di Credito	Tempestiva
7b	Eventuale comunicazione alla Polizia Postale	Amministratore di Sistema	Responsabile CED	Protocollo	Protocollo in partenza		Segnalazione ala Polizia Postale	Polozia Postale	
8	Svolgimento misure adottate	Titolare del trattamento					Risoluzione evento	Titolare del trattamento	
9	Verifica della NON ripetibilità dell'evento	Titolare del trattamento						Titolare del trattamento	
10	Registrazione dell'evento	Responsabile d'ufficio (1); Responsabile CED (2) ; Dirigente						Titolare del trattamento	

(1) limitatamente all'individuazione dei soggetti autorizzati a trattare i dati rispetto alle mansioni svolte.
(2) per la corretta impostazione delle misure di protezione dei sistemi informatici.