COMUNE DI FOSSALTA DI PIAVE

PROVINCIA DI VENEZIA

Documento programmatico-piano operativo per l'adozione delle misure di sicurezza nel trattamento dei dati personali nell'ambito delle attività del Comune.

(Art. 34 comma 1, lett. g) del D.Lgs. n. 196/2003)

Aggiornato all'anno 2011 con deliberazione di Giunta Comunale n. ___ del _____

Piazza IV Novembre n° 5 - c.a.p. 30020 – tel. 0421679644 – fax 0421 679697 – C.F. / P. IVA: 00703420273-e-mail: info@comunefossaltadipiave.it

Indice delle schede

Descrizione delle schede

SCHEDA n. 1: Elenco dei luoghi interessati al trattamento dei dati.
L'analisi dei luoghi è necessaria per individuare quali protezioni sono in uso. Per esempio: se vengono chiuse le porte, se vengono chiusi gli armadi che contengono gli archivi cartacei, se esiste un impianto d'allarme, ecc. Il campo *Scopi* è utilizzato per elencare le funzioni svolte nell'ufficio in aggiunta a quella deducibile dal campo *Descrizione.*. Il campo *Scopi* inoltre elenca eventuali altre attività svolte all'interno dell'ufficio non immediatamente riconducibili al campo *Descrizione.*
All'interno delle altre schede gli uffici sono identificati con la sigla "LF" (Luogo Fisico) seguito dal numero progressivo dell'ufficio stesso.

SCHEDA n. 2: Elenco dei computer presenti all'interno dei vari uffici (il campo *Ufficio* fa riferimento al campo *Descrizione ufficio* della scheda n. 1).
La *Descrizione,* il *Modello* e il *Sistema Operativo* identificano univocamente il computer. Il campo *Descrizione* serve per riconoscere il pc all'interno dell'ufficio. Sono indicate quali password sono in uso su quella macchina oltre alla presenza di software antivirus: il campo *Come RH n.* fa riferimento al codice del computer che accentra la gestione dell'antivirus (da ricerca in questa stessa scheda) viceversa, se non presente, è intesa un'installazione in locale di tale software (in questo caso sono indicati anche il *Tipo* d'antivirus e la *Frequenza aggiornamento* - con il termine "Manuale" si intende l'aggiornamento delle impronte virali eseguito non con cadenza regolare).
All'interno delle altre schede gli uffici sono identificati con la sigla "RH" (Risorsa Hardware) seguito dal numero progressivo del pc stesso.

SCHEDA n. 3: Elenco delle banche dati utilizzate dall'ente.
Sono indicati il nome del responsabile della banca dati e la tipologia degli archivi: se software e/o cartacei.

SCHEDA n. 3a: Dettaglio della banca dati. Numero e descrizione si riferiscono alla scheda n. 3.
La scheda è divisa in 3 parti.

1ª. Contiene informazioni relative all'archivio elettronico: codice del computer che ospita l'archivio (che è il campo *N.* della scheda 2), se viene eseguito il back-up della banca dati, se tale back-up è quello di un computer *x* o, se in locale, il *Tipo backup* (floppy, DAT, ecc.) e la *Frequenza* dello stesso (con il termine "Manuale" si intende il salvataggio della banca dati eseguito non con cadenza regolare)
2ª. Contiene informazioni relative all'archivio cartaceo: *Ubicazione archivio* si riferisce al campo *Descrizione ufficio* della scheda n. 1.
3ª. Elenca l'insieme di dati presenti nell'archivio e il loro tipo: Personale, Sensibile, Giudiziario.

SCHEDA n. 4: Elenco dei trattamenti effettuati nell'ente.
Le informazioni di *Natura dei dati* sono ricavate dalla 3ª parte della scheda n. 3. Con *Struttura principale* è indicato il codice dell'ufficio principale in cui è gestito il trattamento (riferito al campo codice della scheda n. 1) mentre *Struttura secondaria o Esterna* indica l'eventuale ufficio secondario o soggetto esterno che partecipa alla gestione del trattamento (vedi scheda n. 5 - per le struttura secondarie - e scheda n. 10 - per le struttura esterne). L'ultima colonna indica gli eventuali archivi utilizzati.

SCHEDA n. 5: Distribuzione sintetica dei compiti tra strutture principali e secondarie (vedi scheda n. 10 per strutture esterne all'ente). *Ufficio* fa riferimento al campo *Descrizione ufficio* della scheda n. 1 e il codice del trattamento al campo *N.* della scheda n. 4.
Con il termine "Gestione completa" si comprendono tutte le varie modalità di trattamento eseguite da quel ufficio su quel trattamento

SCHEDA n. 6: Dopo l'analisi della scheda n. 1, 2 e 3a per ogni *Elemento di rischio* viene individuata la soglia di rischio e il motivo di tale livello; se un elemento di rischio indica due livelli, per esempio Lieve e Media, significa che la soglia individuata è una via di mezzo tra le due.
La colonna *Rif. 19.4* fa riferimento al campo *Numero* della scheda n. 7.

SCHEDA n. 7: Elenco delle misure da adottare per controbattere le varie soglie di rischio rilevate nella scheda n. 6.
È indicata la data in cui è stata inserita la misura minima, *Compilata il*, e la data da quando tale misura è attiva, *Operativa dal*. La *Tipologia* indica il tipo d'intervento da effettuare:

- ORGANIZZATIVA: misura minima che impartisce istruzioni al personale per correggere comportamenti non precisi.
- LOGICA: misura minima che opera sui programmi, sul software in genere.
- FISICA: misura minima che interviene sui locali e/o uffici.

SCHEDA n. 8: Per ogni banca dati, vedi scheda 3 e 3a, è indicata la frequenza di salvataggio e l'ubicazione delle copie di back-up oltre alla frequenza delle prove di ripristino dei dati e l'ufficio incaricato ad effettuare tali prove. Con il termine "Manuale" si intende la prova di ripristino della banca dati eseguita non con cadenza regolare
Sono riportate solo le banche dati software.

SCHEDA n. 9: Elenco dei corsi previsti per rendere edotto il personale dell'ente. *Tempi previsti* è l'indicazione entro quale data/periodo fare tali corsi.

SCHEDA n. 10: Nel caso in cui sulla scheda n. 4 sia indicata una struttura esterna che partecipa alla gestione del trattamento qui deve essere indicata l'attività svolta da tale soggetto e gli impegni assunti (per esempio in fase di stipula del contratto) o le misure adottate per garantire che i dati personali affidategli siano trattati in modo conforme al Codice. *N.* è il codice del trattamento della scheda n. 4.

Luoghi fisici

Elenco dei luoghi dove viene effettuato il trattamento

Luogo	Indirizzo	Sede	Distaccamento
Municipio	Piazza IV Novembre, 5	☑	☐

Descrizione ufficio		Scopi per cui è usato	Dispositivi di protezione
1 DEMOGRAFICI		URP	
	Note ufficio		
2 TRIBUTI			
	Note ufficio		
3 EDILIZIA/URB.		Manutenzioni	
	Note ufficio	Comunica con LF 4	
4 EDILIZIA/URB.		EDILIZIA PRIVATA, URBANISTICA	
	Note ufficio	2 vani comunicanti tra loro. Comunica con LF 3 e LF 5	
5 LL.PP. 1			
	Note ufficio	2 vani comunicanti tra loro. Comunica con LF 4	
6 LL.PP. 2		Progettazione, direzione lavori	
	Note ufficio	Comunica con LF 7	
7 RESP. LL.PP.			
	Note ufficio	Comunica con LF 6	
8 PERSONALE		ECONOMATO, COMMERCIO, CASA	
	Note ufficio		
9 PROTOCOLLO		GESTIONE ARCHIVIO, CENTRALINO	
	Note ufficio	Comunica con LF 10	
10 RESP. AREA AFF. GENERALI		RAPPORTI CON ALTRI ENTI, BILANCIO	
	Note ufficio	Comunica con LF 9	
11 RAGIONERIA			
	Note ufficio		
12 POLIZIA LOCALE			
	Note ufficio		
13 BIBLIOTECA			
	Note ufficio		
14 ASSESSORI			
	Note ufficio	Comunica con LF 15	
15 SINDACO			
	Note ufficio	Comunica con LF 14 e LF 16	
16 SEGRETERIA		PATTO TERRITORIALE	
	Note ufficio	Comunica con LF 15	
17 CULTURA		PUBBLICA ISTRUZIONE, SPORT	
	Note ufficio		
18 SALA SERVER			
	Note ufficio		

Note del luogo Ingresso principale videosorvegliato ma nessun impianto di allarme periferico. Nessuna protezione sulle finestre al piano terra. Ogni ufficio viene chiuso a chiave oltre l'orario di lavoro.

Risorse hardware

Elenco dei computers utilizzati per il trattamento dei dati

N.	Descrizione	Modello	Sistema operativo	Categoria	Ufficio
1	dominio	xSeries235	Windows XP	Server	Sala server

Password			Antivirus	
bios	rete	screensaver	*Tipo*	*Frequenza aggiornamento*
☐	☑	☑	Symantec antivirus	Automatica

La sede municipale e la sede staccata con l'Ufficio Servizi Sociali sono collegate per il traffico voce e dati, tramite un ponte radio.

Elenco banche dati

Elenco delle banche dati contenenti i dati

N.	*Banca dati*	*Responsabile*	*Software*	*Cartacea*
1	DEMOGRAFICI	Ferrarese Franca	☑	☑
2	PRATICHE EDILIZIE	Finotto Manrico	☑	☑
3	TRIBUTI	Finotto Manrico	☑	☑
4	DELIBERE/DETERMINE/DECRETI	Ferrarese Franca	☑	☑
5	CONTRATTI	Ferrarese Franca	☑	☑
6	CONCESSIONI CIMITERIALI	Ferrarese Franca	☑	☑
7	PERSONALE	Ferrarese Franca	☑	☑
8	COMMERCIO	Ferrarese Franca	☑	☑
9	ERP	Ferrarese Franca	☐	☑
10	PROTOCOLLO	Ferrarese Franca	☑	☑
11	CONTABILITÀ	Ferrarese Franca	☑	☑
12	POLIZIA LOCALE	Milanello Fabrizio	☐	☑
13	BIBLIOTECA	Ferrarese Franca	☑	☑
14	PATTO TERRITORIALE	Zaramella Gianpietro	☐	☑
15	PUBBLICA ISTRUZIONE	Ferrarese Franca	☑	☑
16	SAD	Ferrarese Franca	☑	☑
17	LL.PP.	Finotto Manrico	☑	☑
18	SICUREZZA SUL LAVORO	Zaramella Gianpietro	☐	☑
19	INVENTARIO	Finotto Manrico	☑	☑
20	MANUTENZIONE	Finotto Manrico	☑	☑
21	ELENCO DITTE	Finotto Manrico	☑	☑
22	CONTRIBUTI	Ferrarese Franca	☑	☑
23	SEGRETARIATO SOCIALE	Ferrarese Franca	☐	☑
24	ASSOCIAZIONISMO	Ferrarese Franca	☑	☑
25	URBANISTICA	Finotto Manrico	☑	☑

Risorse dati

Dettaglio delle banche dati

1 DEMOGRAFICI

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ *Si* ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio DEMOGRAFICI

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafiche dei non residenti	☑	☐	☐
Atti di stato civile	☑	☐	☐
Casellario per diritto al voto	☐	☐	☑
Dati dell'elettorale	☑	☐	☐
Liste di leva	☑	☐	☐
Anagrafiche dei cittadini residenti e AIRE	☑	☐	☐

2 PRATICHE EDILIZIE

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ *Si* ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio URBANISTICA

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Dati dell'istruttoria in genere	☑	☐	☐
Anagrafiche intestatari	☑	☐	☐
Dati relativi ai fabbricati	☑	☐	☐

3 TRIBUTI

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ ***No*** ◉ ***Si*** ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio URBANISTICA

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Stato di salute per maggiori detrazioni	☐	☑	☐
Anagrafica degli utenti	☑	☐	☐
Dati degli immobili	☑	☐	☐

4 DELIBERE/DETERMINE/DECRETI

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ ***No*** ◉ ***Si*** ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio SEGRETERIA

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Dati degli atti in genere	☑	☑	☑

5 CONTRATTI

Banca dati Software ☐

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *0*

Backup ◉ ***No*** ○ ***Si*** ***quello della Risorsa Hardware n.*** 0

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio SEGRETERIA

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafica dei contraenti	☑	☐	☐
Dati del contratto in genere	☑	☐	☐

6 CONCESSIONI CIMITERIALI

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ ***No*** ◉ ***Si*** ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio SEGRETERIA

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafica del richiedente	☑	☐	☐
Stato di salute per diritto seconda fila	☐	☑	☐

7 PERSONALE

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ *Si* ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio PERSONALE

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Iscrizione a sindacati	☐	☑	☐
Casellario giudiziario	☐	☐	☑
Stato di salute	☐	☑	☐
Dati personali del dipendente	☑	☐	☐
Dati sul trattamento economico	☑	☐	☐

8 COMMERCIO

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ *Si* ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio PERSONALE

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafiche degli esercizi	☑	☐	☐
Dati sull'attività	☑	☐	☐

9 ERP

Banca dati Software ☐

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *0*

Backup ◉ *No* ○ *Si* ***quello della Risorsa Hardware n.*** 0

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio PERSONALE

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafica richiedenti o assegnatari	☑	☐	☐
Dati economici dei richiedenti o degli inquilini	☑	☐	☐
Stato di salute ai fini della graduatoria	☐	☑	☐

10 PROTOCOLLO

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ *Si* ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio PROTOCOLLO

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafica mittenti/destinatari	☑	☐	☐
Oggetti diversi della corrispondenza	☑	☑	☑

11 CONTABILITÀ

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ ***Si*** ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio RAGIONERIA

Note

Tipi di dati contenuti nell'archivio	***Personale***	***Sensibile***	***Giudiziario***
Anagrafica debitori/creditori	☑	☐	☐
Dati del bilancio	☑	☐	☐
Dati dell'economato	☑	☐	☐
Dati dell'IVA	☑	☐	☐

12 POLIZIA MUNICIPALE

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ ***Si*** ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio POLIZIA MUNICIPALE

Note

Tipi di dati contenuti nell'archivio	***Personale***	***Sensibile***	***Giudiziario***
Segnalazioni e notifiche da altri enti	☑	☑	☑
Accertamenti di igiene ambientale	☑	☐	☑
Contravvenzioni e incidenti stradali	☑	☑	☑

13 BIBLIOTECA

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ ***No*** ◉ ***Si*** ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio BIBLIOTECA

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafica utenti	☑	☐	☐
Convinzioni religiose e politiche	☐	☑	☐

14 PATTO TERRITORIALE

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ ***No*** ◉ ***Si*** ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio PATTO TERRITORIAL

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafiche beneficiari dei contributi	☑	☐	☐

15 PUBBLICA ISTRUZIONE

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ ***No*** ◉ ***Si*** ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio CULTURA

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafica utenti	☑	☐	☐
Dati sensibili per utenti della mensa	☐	☑	☐

16 SAD

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *2*

Backup ◉ ***No*** ○ ***Si*** ***quello della Risorsa Hardware n.*** 0

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio SERVIZI SOCIALI

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafiche utenti	☑	☐	☐
Dati degli interventi domiciliari	☑	☐	☐
Dati sulla salute	☐	☑	☐

17 LL.PP.

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ ***No*** ◉ ***Si*** ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio LL.PP.

Note

Tipi di dati contenuti nell'archivio	***Personale***	***Sensibile***	***Giudiziario***
Anagrafica dei progettisti	☑	☐	☐
Anagrafiche direttori dei lavori	☑	☐	☐
Anagrafica delle ditte	☑	☐	☐
Anagrafica del responsabile della sicurezza	☑	☐	☐
Categoria dei lavori	☑	☐	☐
Dati dell'opera (date inizio/fine lavori, importi, ecc.)	☑	☐	☐

18 626

Banca dati Software ☐

Banca dati Cartacea ☐

Archivio elettronico

Risorsa Hardware ospite n. *0*

Backup ◉ ***No*** ○ ***Si*** ***quello della Risorsa Hardware n.*** 0

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio

Note

Tipi di dati contenuti nell'archivio	***Personale***	***Sensibile***	***Giudiziario***
Anagrafica dipendente	☑	☐	☐
Stato di salute	☐	☑	☐

19 INVENTARIO

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ *Si* ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio LL.PP.2

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Dati degli immobili	☑	☐	☐
Dati dei beni mobili	☑	☐	☐

20 MANUTENZIONE

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ *Si* ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio LL.PP.

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Anagrafica ditte manutentrici	☑	☐	☐

21 ELENCO DITTE

Banca dati Software ☐

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *0*

Backup ◉ *No* ○ *Si* ***quello della Risorsa Hardware n.*** 0

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio LL.PP.

Note *Altri uffici interessati*

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Elenco ditte fornitori dei lavori pubblici	☑	☐	☐
Elenco ditte richiedenti partecipazione a trattativa privata	☑	☐	☐

22 CONTRIBUTI

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ *Si* ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio SERVIZI SOCIALI

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Situazione reddittuale	☑	☐	☐
Stato di salute ai fini della graduatoria	☐	☑	☐
Anagrafica richiedenti	☑	☐	☐

23 SEGRETARIATO SOCIALE

Banca dati Software ☐

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *0*

Backup ◉ *No* ○ *Si* ***quello della Risorsa Hardware n.*** 0

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio SERVIZI SOCIALI

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Stato di salute	☐	☑	☐
Dati economici	☑	☐	☐
Segnalazioni in arrivo da altri enti	☑	☑	☑
Anagrafica utente	☑	☐	☐

24 ASSOCIAZIONISMO

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ *No* ◉ *Si* ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio CULTURA

Note

Tipi di dati contenuti nell'archivio	*Personale*	*Sensibile*	*Giudiziario*
Elenco associazioni	☑	☐	☐

25 URBANISTICA

Banca dati Software ☑

Banca dati Cartacea ☑

Archivio elettronico

Risorsa Hardware ospite n. *1*

Backup ○ ***No*** ◉ ***Si*** ***quello della Risorsa Hardware n.*** 1

Tipo backup ***Frequenza backup***

Note

Archivio cartaceo

Ubicazione archivio URBANISTICA

Note

Tipi di dati contenuti nell'archivio	***Personale***	***Sensibile***	***Giudiziario***
Destinazione delle aree	☑	☐	☐
Dati catastali in genere	☑	☐	☐
Dati delle proprietà oggetto dell'intervento	☑	☐	☐

Elenco dei trattamenti (regola 19.1)

Trattamenti effettuati dal titolare, direttamente o attraverso collaborazioni esterne, con l'indicazione della natura dei dati e della struttura interna o esterna preposta.

N.	*Descrizione sintetica*	*Natura dei dati*		*Struttura principale*	*Struttura secondaria o esterna*	*Archivi utilizzati*
		Sensibili	*Giudiziari*			
1	Gestione degli atti amministrativi	☑	☑	6	10, tutti	4 – 6
2	Nucleo di valutazione	☐	☐	7	Responsabili	
3	Gestione giuridica ed economica del personale	☑	☑	7		7
4	Sicurezza sul lavoro	☑	☐	7		18
5	Rilascio autorizzazioni, concessioni, permessi certificazioni, licenze	☐	☐	7, 4		8 – 2
6	Gestione degli alloggi ERP	☑	☐	7	Poste Italiane	9
7	Gestione dei servizi demografici, censimenti e statistiche	☑	☐	1	tutti	1
8	Servizi al cittadino, front-office	☐	☐	1		
9	Progettazione e attività amministrativa dei lavori pubblici	☐	☐	5	3	17-21
10	Gestione e aggiornamento inventario dei beni	☐	☐	5, 7		19
11	Gestione e manutenzione del patrimonio comunale	☐	☐	2		20
12	Raccolta domande ed erogazione contributi	☑	☐	18	10	22
13	Gestione casi sociali	☑	☑	18	10, 11	23
14	Gestione interventi domiciliari	☑	☐	18		16
15	Gestione servizi scolastici	☑	☐	16	10	15
16	Organizzazione attività culturali	☐	☐	16	10	24
17	Gestione attività sportive e ricreative	☐	☐	16	10	24
18	Gestione della biblioteca	☑	☐	12		13
19	Pianificazione urbanistica e controllo del territorio	☐	☐	4	11	25
20	Gestione dei tributi e attività di accertamento	☑	☐	4	Equitalia, Poste Italiane	3

N.	*Descrizione sintetica*	*Natura dei dati* *Sensibili*	*Giudiziari*	*Struttura principale*	*Struttura secondaria o esterna*	*Archivi utilizzati*
21	Gestione del protocollo	☑	☑	8	tutti	10
22	Gestione economico-finanziaria dell'ente	☐	☐	10	CARIVE	11
23	Assistenza alle imprese nella gestione dei contributi dello stato	☐	☐	15		14
24	Gestione del contenzioso	☐	☐	9		
25	Gestione delle assicurazioni	☐	☐	9		
26	Gestione contravvenzioni incidenti	☑	☑	11		12
27	Gestione notifiche e segnalazioni da altri enti	☑	☑	11		12
28	Gestione interventi ecologici e ambientali	☐	☑	11		12

Distribuzione compiti (regola 19.2)

Elenco dei compiti per ufficio in relazione ai trattamenti effettuati

Ufficio	*Trattamenti*	*Compiti/Gestione/Operazioni*
SEGRETERIA	1	Gestione completa
TUTTI	1	Istruttoria preliminare dei contratti e stesura atti preparatori di propria competenza
RAGIONERIA	1	Gestione economica dei contratti e concessioni
PERSONALE	2-6	Gestione completa
RESPONSABILI	2	Servizio di controllo interno
PERSONALE	6	Attività previste dalla legge su alloggi ATER
DEMOGRAFICI	7	Gestione completa
TUTTI	1, 7, 21	Consultazione
RESP. AREA LL.PP.	9	Attività di coordinamento
LL.PP.2	9	Gestione completa
LL.PP.2	10	Gestione e manutenzione dei beni immobili
PERSONALE	10	Gestione dei beni mobili
LL.PP.	11	Gestione completa
SERVIZI SOCIALI	12-13	Gestione completa
RAGIONERIA	12-13, 15	Emissione dei mandati
POLIZIA MUNICIPALE	13	Attività di supporto all'intervento
CULTURA	15	Gestione completa
BIBLIOTECA	18	Gestione completa
PERSONALE	5	Attività connessa al rilascio di autorizzazioni del commercio
URBANISTICA	5	Attività connessa al gestione dell'edilizia privata
URBANISTICA	19-20	Gestione completa
POLIZIA MUNICIPALE	19	Sopralluoghi congiunti
PROTOCOLLO	21	Gestione completa
RAGIONERIA	22	Gestione completa
PATTO TERRITORIALE	23	Gestione completa
RESP. AREA AFFARI GEN	24-25	Gestione completa
POLIZIA MUNICIPALE	26-28	Gestione completa

Elementi di rischio (regola 19.3)

Individuazione degli elementi di rischio che minacciano i dati

Risorsa	*Elemento di rischio*	*Soglia individuata* Lieve	Media	Grave	*Motivo*	*Rif. 19.4*
Luoghi fisici	Possibilità d'intrusione	☑	☐	☐	Nessun allarme a protezione dei locali	1
Luoghi fisici	Allagamenti	☑	☐	☐	Zona non soggetta	
Luoghi	Incendio	☑	☐	☐	Realizzato impianto antincendio a gas nella zona adibita ad archivi	2
Luoghi	Furto	☑	☐	☐	Porte chiuse regolarmente in assenza del personale dell'ufficio	
Hardware	Uso non autorizzato dell'hardware	☑	☐	☐	Né BIOS né di screen saver. Password di accesso ad internet	3
Hardware	Manomissione/Sabotaggio	☑	☐	☐	Porte sempre chiuse. Stanza server chiusa	4
Hardware	Probalità/frequenza di guasto	☑	☐	☐	Pc di recente acquisto	
Hardware	Intercettazione trasmissioni	☑	☐	☐	Firewall e proxy a protezione della rete	3
Hardware	Rischi connessi all'elettricità	☑	☐	☐	Rete stabile-presenza di gruppo di continuità	8
Dati software	Accesso non autorizzato	☑	☐	☐	Password di rete	
Dati cartacea	Accesso non autorizzato	☑	☑	☐	Manca il registro degli accessi	4
Dati software	Cancellazione/Manomissione software non autorizzata di dati	☑	☐	☐	Profili assegnati agli operatori e password d'accesso per le procedure	
Dati cartacea	Cancellazione/Manomissione	☑	☑	☐	Armadi aperti	5
Dati software	Perdita di dati	☑	☐	☐	Back-up con 7 cassette (di cui 1 settimanale e 1 mensile)	7
Dati cartacea	Perdita di dati	☑	☑	☐	Il rischio principale rimane l'incendio	2
Dati	Incapacità di ripristinare copie di sicurezza	☑	☐	☐	Prove periodiche di riprisitno	6
Dati	Virus	☑	☐	☐	Antivirus centralizzato aggiornato	
Dati	Presenza di codice non conforme	☑	☐	☐	Nessuna scansione manuale dei vari dischi fissi	7

Misure minime (regola 19.4)

Misure programmatiche per bilanciare gli elementi di rischio

Numero	*Tipologia*	*Descrizione*	*Compilata il*	*Operativa dal*
1	FISICA	Installare un sistema d'allarme volumetrico a protezione dell'intero stabile	28/03/2008	
2	FISICA	Considerata la mancanza di un sistema di rilevamento fumi, prevedere l'acquisto di armadi ignifughi almeno per gli uffici che trattano dati sensibili e giudiziari	28/03/2008	
3	LOGICA	Inserire la password di BIOS e di screen saver su ogni PC per evitare, con la prima, l'uso non autorizzato del PC in orario di chiusura dell'ufficio e con la seconda l'uso improprio del PC durante l'assenza dell'incaricato	28/03/2008	
4	ORGANIZZATIVA	Creare il registro degli accessi ai locali oltre l'orario di chiusura per monitorare gli accessi agli uffici contenenti dati sensibili	28/03/2008	
5	ORGANIZZATIVA	Impartire istruzioni per la chiusura corretta degli armadi contenenti dati sensibili e giudiziari	28/03/2008	
6	ORGANIZZATIVA	Pianificare delle prove di ripristino periodiche dei dati da cassetta almeno con cadenza bimensile	28/03/2008	
7	ORGANIZZATIVA	Impartire istruzioni agli incaricati perché eseguano la scansione manuale del disco fisso del proprio PC per rilevare codici non conformi o dannosi (virus o altro), almeno con cadenza mensile	28/03/2008	

Disponibilità dei dati (regola 19.5)

Frequenza di salvataggio e di ripristino delle banche dati

N. banca dati	*Frequenza di salvataggio*	*Ubicazione copie*	*Frequenza ripristino*	*Ufficio incaricato*
Tutti	Giornaliera	8	Nessuna	8

Criteri per il ripristino dei dati:

7 cassette di cui:
- 5 giornaliere
- 1 settimanale (sabato)
- 1 mensile (ultimo sabato del mese)

Interventi formativi (regola 19.6)

Pianificazione dell'attività formativa

N.	*Descrizione intervento*	*Destinatari*	*Tempi previsti*
1	Consegna documento "Privacy – Linee Guida"	TUTTI	consegnato dicembre 2005
2	Consegna istruzioni richieste dall'Allegato B	TUTTI	consegnato dicembre 2005

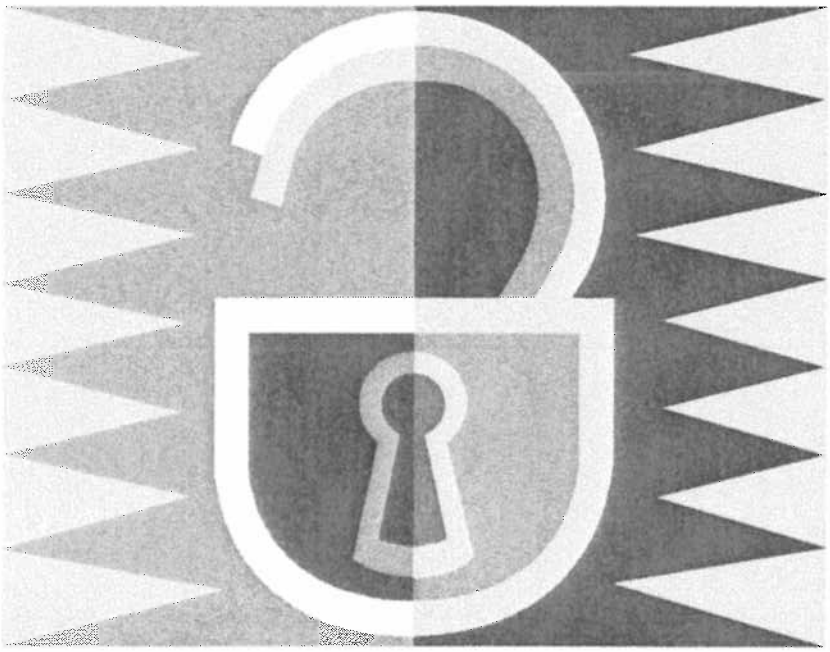
Trattamenti esterni (regola 19.7)

Elenco dei trattamenti affidati all'esterno

N.	*Attività svolta*	*Soggetto esterni*	*Impegni assunti/misure adottate*
20	Attività di riscossione	Equitalia	Come da contratto stipulato
6, 20	Attività di riscossione	Poste Italiane	Come da contratto stipulato
22	Attività di riscossione e pagamento	Cassa di Risparmio di Venezia	Come da contratto stipulato

Privacy

Linee guida



versione 2

Sommario

Premessa

Questo documento fornisce una panoramica sulle responsabilità che derivano dal rispetto della "sicurezza" e detta alcune norme base di comportamento.

Nell'ambito informatico, il termine "sicurezza" si riferisce a:

- **Riservatezza**: Prevenzione contro l'accesso non autorizzato alle informazioni;
- **Integrità**: Le informazioni non devono essere alterabili da incidenti, abusi o codice dannoso;
- **Disponibilità**: Il sistema deve essere protetto da interruzioni impreviste.

Questi 3 aspetti rappresentano gli obiettivi il cui raggiungimento richiede non solo l'utilizzo d'appropriati strumenti tecnologici, ma anche d'opportuni meccanismi organizzativi; misure soltanto tecniche, per quanto possano essere sofisticate, non saranno efficienti se non usate in modo appropriato.

In particolare, le precauzioni di tipo tecnico possono proteggere le informazioni durante il loro transito attraverso i sistemi, o anche quando queste rimangono inutilizzate su un disco di un computer; nel momento in cui esse raggiungono, o sono raggiunte da, l'utente finale, la loro protezione dipende esclusivamente da questo ultimo, e nessun strumento tecnologico può sostituirsi al suo senso di responsabilità e rispetto delle norme.

Competenze

Chiunque, a qualsiasi livello, rientra in una o più d'una di queste figure.

Titolare del trattamento, Compiti del

Esercita potere decisionale sulle finalità e modalità di trattamento.

Nomina di Responsabili del trattamento e l'Amministratore di sistema.

Impartisce le istruzioni come richiesto dalle regole 4, 9, 10, 18, 21, 23, 27 dell'AllegatoB "Disciplinare tecnico in materia di misure minime di sicurezza".

Responsabile del trattamento, Compiti del

Provvedere all'adattamento specifico, per le esigenze dell'ufficio, del Documento programmatico sulla sicurezza (d'ora in poi DPS).

Provvedere all'effettiva realizzazione di quanto indicato nel DPS.

Provvedere alla salvaguardia delle banche dati affidategli.

Nominare gli incaricati.

Incaricato del trattamento, Compiti del

Attenersi alle istruzioni impartite dal Titolare o dal Responsabile

Rispettare le disposizioni contenute nel presente documento.

Amministratore di sistema, Compiti del

Svolgere materialmente le operazioni necessarie a garantire il funzionamento del sistema informatico, sotto la direzione del titolare.

Attivare le nuove utenze e, contestualmente alla comunicazione di nome utente e password, consegnare ai nuovi utenti il presente documento.

Verificare almeno una volta al mese l'elenco delle persone autorizzate ad accedere agli archivi.

Mettere in atto tutte misure minime di sicurezza individuate nel DPS relative alla gestione delle parole chiave.

Mantenere l'elenco delle password dei vari utenti.

[N.B.] Si ricorda che questa non è una figura espressamente richiesta dal Codice della privacy ma se ne deriva la nomina dall'analisi dei compiti richiesti in materia di protezione di dati trattati con strumenti elettronici.

Definizioni

Dati personali
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
Dati personali idonei a rivelare l'originale razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Dati giudiziari
I dati personali idonei a rivelare provvedimenti di cui all'articolo 3 comma 1, lettere da a) a o) e da r) a u), del DPR 14 novembre 2002 n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Dati identificativi
I dati personali che permettono l'identificazione diretta dell'interessato.

Trattamento
Qualunque operazione o complesso di operazioni, effettuati anche 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, 1'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

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.

Banca dati
Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

Misure minime
Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31.

Misure di sicurezza già in essere

- Ogni incaricato provvede alla periodica sostituzione della propria parola chiave, previa comunicazione al soggetto preposto alla custodia delle parole chiave.

- I codici identificativi personali per l'utilizzo del pc sono assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi.

- E' vietato l'utilizzo di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.

- Il programma in dotazione contro il rischio di danneggiamento, l'antivirus, è aggiornato con cadenza almeno settimanale.

- Periodicamente, e in ogni caso almeno una volta l'anno, è verificata la sussistenza delle condizioni per le autorizzazioni all'accesso alle varie banche dati. (L'autorizzazione all'accesso deve in ogni caso intendersi limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione.)

- È stato predisposto, e sarà aggiornato con cadenza annuale entro il 31 marzo d'ogni anno, il DPS.

L'accesso alla sala server ovvero al luogo dov'è custodito il server, è consentito solo alle persone espressamente autorizzate.

In assenza del personale autorizzato, la sala server deve essere tenuta chiusa a chiave.

Tutte le chiavi vanno custodite dal personale delegato dal Responsabile del servizio.

Criteri e procedure per assicurare l'integrità dei dati

Presso ciascun ufficio è consentita l'installazione esclusiva della seguente categoria di software:

- Software commerciale dotato di licenza d'uso;
- Software *open source* dotato di licenza GPL;

L'installazione di software diversi da quelli indicati va autorizzato dal titolare o, se designato, dall'amministratore di sistema. La conformità del software viene di norma certificata dall'ufficio CED. Il software deve essere installato solo da supporti fisici originali o dei quali è nota la provenienza.

L'ufficio CED provvede, ove mancante, alla distribuzione e installazione di un software antivirus aggiornato.

In mancanza di procedure di aggiornamento automatiche, il responsabile del trattamento si preoccupa di garantire l'effettuazione degli aggiornamenti del software antivirus su tutte le postazioni di lavoro utilizzate per effettuare i trattamenti a lui assegnati, con cadenza almeno settimanale.

Integrità dei dati

L'amministratore di sistema, con la collaborazione dei vari responsabili d'ufficio, mantiene un elenco, aggiornabile all'occorrenza, di tutte le risorse hardware dell'ufficio.

Ogni responsabile di trattamento individua i volumi logici o le aree di disco da sottoporre a backup.

A ciascun utente viene assegnata una directory, in un'area disco di un server che sia sottoposta a backup, dove registrare i dati che debbono essere mantenuti in maniera sicura. L'accesso a queste directory è consentita esclusivamente all'utente proprietario, nonché agli incaricati del backup.

Il Titolare del trattamento individua uno o più incaricati del backup.

Laddove il backup venga effettuato localmente nell'ambito dell'ufficio, gli incaricati effettuano le seguenti operazioni:

- Esecuzione quotidiana del backup, possibilmente attraverso procedure automatiche;
- Verifica della corretta esecuzione dei backup;
- Tenuta di un elenco dei backup effettuati;
- Verifica, con cadenza almeno mensile, della procedura di recovery dai supporti di backup;
- Effettivo ripristino dei dati in caso di necessità.

Controllo degli accessi

Tutte le stazioni di lavoro debbono essere protette da una password di accensione (password BIOS) e da una password d'accesso alla rete (password di rete).

La password di BIOS va modificata con cadenza annuale.

L'inserimento della password di BIOS va effettuato a cura dell'utente, affidandone una copia, al responsabile incaricato che le custodirà sotto chiave. Ai fini dell'assistenza sistemistica, la password di accensione può venire comunicata agli incaricati e sostituita al termine dell'intervento.

Il *Responsabile* fornisce ai preposti alla custodia delle parole chiave i nominativi e la qualifica degli utenti autorizzati, nonché i loro privilegi di utilizzo del sistema informatico. I preposti provvedono:

- A definire, per ciascun utente, il nome utente e la password per il primo accesso;
- A consegnare agli interessati il nome utente e la password, unitamente a una copia del presente documento;

Dove questo è tecnicamente possibile, i preposti alla custodia delle parole chiave impostano il sistema in modo da forzare l'utente:

- A cambiare la password periodicamente, con una frequenza non superiore a 6 mesi;
- A non poter utilizzare lo stesso nome utente per accedere contemporaneamente al sistema da due postazioni di lavoro distinte.

Trasmissione dei dati

Le connessioni telematiche da e verso le banche dati degli uffici sono distinti in tre categorie:

1. Connessioni provenienti da altri uffici dell'Amministrazione;
2. Connessioni effettuate dall'interno dell'Amministrazione su postazioni di lavoro pubblicamente disponibili;
3. Connessioni effettuate tramite modem da postazioni collegate alla rete dell'ufficio.

Qualora siano necessarie connessioni del tipo descritto al precedente punto 3, queste andranno effettuate da risorse hardware dedicate. Per queste risorse hardware andranno previste adeguate misure di controllo degli accessi.

Piano di intervento e formazione

L'amministratore di sistema provvede a informare tempestivamente i responsabili del trattamento di ogni eventuale problema di sicurezza di cui dovesse venire a conoscenza.

I soggetti responsabili del trattamento provvederanno a informare tempestivamente gli incaricati:

- della presenza di virus negli elaboratori dell'ufficio;
- di prassi non conformi da parte del personale alle disposizioni di sicurezza;
- della periodica necessità di variazione delle parole chiave da parte degli incaricati;
- della disponibilità di programmi di aggiornamento relativi all'antivirus.

I responsabili, ove richiesto o ove se ne ravvisi la necessità, provvederanno ad organizzare riunioni per l'illustrazione e la diffusione degli accorgimenti da adottare in tema di sicurezza.

Linee guida relative ai virus

Cos'è un virus

Un virus è un programma in grado di trasmettersi autonomamente e che può causare effetti dannosi quali:

- rallentare l'esecuzione dei programmi o del sistema operativo;
- modificare i comportamenti originali dei programmi installati, (es. inviando informazioni riservate via rete, disattivando eventuali protezioni di sicurezza, ecc.);
- distruggere o modificare arbitrariamente i dati dei file (eseguibili, documenti, immagini, ecc.);
- cercare di replicarsi via rete o tramite supporti (dischetti, dischi rigidi, CD-ROM, ecc.), sfruttando spesso bachi nella sicurezza dei sistema operativo, es. al momento dell'attivazione di un programma, della sua copia, ecc.

Come sono classificati

Dal punto di vista tecnico esistono tre classi principali associabili al generico termine di *virus informatico.*

Virus

Questi insiemi di istruzioni possono infettare i file del programma, i settori di avvio dei sistemi operativi, ecc. e, in genere, si attivano e si replicano solo in seguito a determinate azioni dell'ignaro utilizzatore (esecuzione di programmi infetti, copia di dischetti infettati, ecc.); possono essere molto pericolosi quando cancellano o modificano arbitrariamente i file utente o del sistema operativo ospite.

Vermi (*worm*)

Questi insiemi di istruzioni, dopo essere stati attivati la prima volta (con un programma infetto o con un programma "Troiano"), si autoreplicano attraverso le reti di computer senza bisogno di interventi manuali da parte di ignari utilizzatori; di solito il loro principale effetto è quello di rallentare e, a volte, anche bloccare i sistemi operativi infettati oppure di saturare/intasare le reti di comunicazione.

Troiani (*trojan*)

Questi sono *programmi definiti come maliziosi/malvagi* (malicious code) in quanto sotto le apparenti spoglie di programmi di utilità o giochi si nascondono delle istruzioni (volutamente inserite dagli autori di tali programmi) in grado di trasmettere via internet informazioni riservate del sistema, di attivarsi a comando per attaccare siti internet, di fare danni al sistema dei file o di attivare a loro volta l'esecuzione di virus, vermi, ecc.; la loro pericolosità è molto elevata perchè possono agire silenziosamente

nell'ombra anche per mesi o anni dato che non essendo virus non sono facilmente intercettati dai programmi anti-virus.

I virus possono essere classificati anche in base alle loro principali caratteristiche, es.:

virus *stealth*
virus che cercano di nascondersi dai tentativi di rilevazione o sottrarsi ai tentativi di rimozione;

virus *polimorfici*
virus che appaiono in modo diverso in ogni file infettato, rendendo più difficile la loro individuazione;

virus *multivalenti*
virus che agiscono in molti modi diversi contemporaneamente, es. infettando il settore di avvio, i file programma, ecc.

Si dividono poi in diverse categorie, ognuna caratterizzata da particolari effetti; le principali sono le seguenti.

Virus di programma
Questi virus infettano i file di programma o di sistema che hanno particolari estensioni (es. per sistemi DOS/Windows):

- **.com**
- **.dll**
- **.doc**
- **.dot**
- **.exe**
- **.ppt**
- ecc.

Vedere l'apposita lista nel proprio programma anti-virus.

Virus di avvio
Questi virus infettano aree su disco riservate al BIOS. o al sistema operativo (aree non occupate da file); dato che in queste aree sono registrate le istruzioni di avvio/partenza di un sistema operativo, questi virus sono riattivati automaticamente durante le operazioni di partenza di un sistema oppure durante le operazioni di lettura/copia di dati da un disco all'altro.

Virus di macro/linguaggi interpretati
Questi virus possono infettare qualsiasi documento o programma che contenga o possa eseguire istruzioni scritte in vari linguaggi:

- macro specializzate dipendenti da un particolare programma (es. Lotus Notes, ecc.);
- VBA (Visual Basic for Applications), tutti i documenti MS-Office (Word, Excel, Power Point, Access, ecc.);
- VBS (Visual Basic Script, variante di VBA), usato specialmente nei programmi Microsoft che gestiscono posta (Outlook) o visualizzano pagine Web (Internet Explorer), ecc.
- PHP (linguaggio per pagine web dinamiche);
- Java (linguaggio relativamente indipendente dalla piattaforma usato per applicazioni Internet, es. *applet*, ecc.);
- ecc.

La pericolosità è connessa con l'esecuzione automatica di queste istruzioni dopo un'azione utente (apertura di un documento Word, Excel, animazioni, pre-visualizzazioni automatiche degli allegati di posta elettronica, ecc.).

Virus finti o burla (*hoax*)

Questi non sono dei veri virus, bensì dei messaggi tipo *catena di S. Antonio* che segnalano notizie particolari (presenza di altri virus, barzellette, ecc.) da ritrasmettere urgentemente al maggior numero di persone possibile per informarle dell'oggetto in questione prima che accada qualcosa di grave o irreparabile. Tipicamente si trasmettono tramite messaggi di posta elettronica (e-mail) e il loro stesso moltiplicarsi provoca dei disagi (rallentamento/intasamento dei server di posta elettronica, delle reti di comunicazione, ecc.).

NON DIFFONDETE MESSAGGI DI PROVENIENZA DUBBIA

Quindi se ricevete messaggi che avvisano di un nuovo virus pericolosissimo, ignoratelo: le mail di questo tipo sono, appunto, *hoax* (termine spesso tradotto in italiano con "bufala"), l'equivalente delle "leggende metropolitane" della rete. Questo è vero anche se il messaggio proviene dal vostro migliore amico, dal vostro capo, da vostra sorella o da un tecnico informatico. È vero anche e soprattutto se si fa riferimento a "una notizia proveniente dalla Microsoft" oppure da un'altra casa importante (sono gli *hoax* più diffusi).

Analogamente, tutti i messaggi che vi invitano a "diffondere la notizia quanto più possibile" sono *hoax*. Anche se parlano della fame nel mondo, della situazione delle donne negli stati arabi, di una bambina in fin di vita, se promettono guadagni miracolosi o grande fortuna; sono tutti *hoax* aventi spesso scopi molto simili a quelli dei virus, cioè utilizzare indebitamente le risorse informatiche. Queste attività sono vietate dagli standard di Internet e contribuire alla loro diffusione può portare alla disattivazione/termine del proprio accesso oltre agli effetti indicati in precedenza.

Come si diffondono

Un **virus** si diffonde con il meccanismo della replicazione che si attua in uno dei seguenti modi.

Replicazione via esecuzione / copia di programmi infetti

Questo è il metodo classico utilizzato dalla maggioranza dei virus:

1. l'utente esegue/attiva un programma in cui è contenuto un virus;
2. il virus nascosto è eseguito e, a questo punto, cerca di:
   - installarsi in memoria per intercettare le chiamate di sistema, es. copia file, esecuzione altri programmi;
   - modificare altri programmi / file dati per danneggiarli o per replicare se stesso (es. inserendosi entro spazi vuoti / non usati dei programmi eseguibili);
   - modificare il settore di avvio dei dischi rigidi o dei dischetti removibili per eseguire se stesso all'avvio del sistema non appena il dischetto infetto è acceduto dal sistema operativo (es. lista di file, navigazione all'interno delle cartelle, ecc.);
3. l'utente copia inconsapevolmente i file / programmi infetti su altri supporti (dischi di rete, dischetti, nastri, ecc.) e, non appena qualcuno attiva i programmi infettati o utilizza i supporti infettati in un altro computer, il virus si riattiva e il ciclo di replicazione ricomincia.

Naturalmente i sopracitati passi possono essere eseguiti nei modi più subdoli a seconda delle caratteristiche dei sistemi operativi ospiti.

Replicazione via allegati E-MAIL

Questo metodo sfrutta i punti deboli dei programmi di posta elettronica assieme alle ingenuità tipiche (causa atteggiamento rilassato, fiducioso, ecc.) commesse dall'utilizzatore medio della posta elettronica via internet:

1. l'utente riceve un messaggio di posta elettronica cui è stato allegato un file programma binario o di macro contenente il virus; tale programma può anche essere mascherato (es. con doppia o tripla estensione, con un'icona modificata, ecc.) per somigliare a innocui tipi di file, es. immagini, documenti Word, file zip, ecc.;
2. l'utente "apre" l'allegato di posta; a questo punto il sistema operativo o un componente del programma di posta provvede ad eseguirlo (direttamente o con un apposito programma interprete);
3. il virus fa dei danni o comunque cerca di modificare i programmi di posta e/o di navigazione su Internet per inviarsi automaticamente verso altre destinazioni (es. come allegato a tutti i messaggi trasmessi dall'ignaro utente).
   N.B. Attualmente questo è il metodo più usato dai virus per replicarsi.

Replicazione tramite servizi web

Questo metodo sfrutta i punti deboli sia dei programmi *server* web (es. httpd, ftpd, ircd, ecc.) sia dei programmi *client* che utilizzano tali servizi (es. web *browser*, irc, chat, ecc.). Questo meccanismo è utilizzato da virus particolarmente aggressivi che incorporano sia parti tipiche di un **worm** che quelle classiche per i programmi utente; un meccanismo molto frequente è il seguente:

1. un **worm** si diffonde via rete locale o Internet e, da un computer *server* già infettato, cerca di attaccare altri computer *server* sfruttando i punti deboli di eventuali programmi *server* (es. web server, ecc.) in esecuzione;
2. un comune utente visualizza le pagine web, ospitate nel computer *server* infetto, con un *browser* (es. Microsoft Internet Explorer) che abbia falle nella sicurezza note al creatore del virus e che non siano ancora state corrette tramite un aggiornamento / correzione (*patch*) del programma stesso fornita dal costruttore / fornitore;
3. a questo punto il virus presente nel computer *server* cerca di inserire nelle pagine web visitate dal *browser* del codice *script* (es. VB script, Java, ecc.) o comunque attiva una sequenza di operazioni che possa essere eseguita dal *browser bacato* in modo da prenderne il controllo;
4. una volta acquisito il controllo di un programma *client*, il virus esplica i suoi effetti nella nuova macchina ospite, cercando ovviamente di replicarsi tramite svariati meccanismi (via E-MAIL, ecc.).

Un **verme** (worm) si diffonde quindi con il meccanismo della auto-replicazione via rete (locale o internet), sfruttando punti deboli o bachi dei sistemi operativi interessati, senza bisogno di interventi umani (eccetto che per la prima attivazione).

Che effetti producono

Premesso che per definizione **non esistono virus innocui**, si possono elencare i seguenti effetti:

- insicurezza a causa della loro stessa presenza;
- perdite di tempo/produttività per procedere alla loro eliminazione;
- costi per l'acquisto e l'azionamento di appositi programmi anti-virus;
- rallentamenti o bloccaggi nell'esecuzione dei programmi;
- possibili utilizzi impropri dei computer infettati (chiamati zombie) in modo da farli partecipare ad attacchi DoS eseguiti via internet a danno di server web, ftp, ecc. con conseguenti sovraccarichi della rete e altri oneri causati dal traffico improprio. DoS è l'acronimo di Denial of Service: un particolare tipo di attacco caratterizzato da un esplicito tentativo di prevenire l'uso di un servizio da parte degli utenti interessati);
- possibile diffusione di dati segreti (se questi sono trasmessi via internet);
- perdita di dati, programmi, impostazioni varie;
- eventuale necessità di reinstallare il sistema operativo, e i programmi infettati;
- eventuali spiacevoli responsabilità o danni alla propria immagine nel caso di trasmissione involontaria dovuta a negligenze nei controlli anti-virus.

Gli eventuali danni apportati al sistema dei file possono essere:

- evidenti e/o estesi;
- lenti e impercettibili; questo è forse il caso più pericoloso perché produce danni senza che gli utilizzatori se ne accorgano.

Metodi per evitare o limitare i danni dei virus

Un ente che è dotato di una rete di pc, che comunica con l'esterno via internet e che scambia dati con vari tipi di supporti removibili, non può raggiungere un grado di protezione contro i virus del 100%; tuttavia, applicando costantemente le seguenti regole e utilizzando gli strumenti giusti è possibile avvicinarsi molto alla sicurezza massima richiesta.

La norma generale è la seguente:

1. **Usare sempre un programma anti-virus aggiornato** (es. con aggiornamento automatico giornaliero via internet oppure con aggiornamento manuale almeno settimanale).
2. **Mantenere sempre attivo il programma anti-virus**, specialmente se non si è attenti al contesto in cui si opera, anche se, in teoria, dovrebbe essere sufficiente attivarlo solo quando si scambiano dati / file con l'esterno, es.:
   - quando si leggono supporti removibili (dischetti, CD, ecc.);
   - quando si accede a dischi di rete;
   - quando si scambiano dati via rete internet (posta elettronica o anche la semplice navigazione su pagine Web).

Si noti che i programmi anti-virus sempre attivi occupano una discreta quantità di memoria (RAM) e rallentano considerevolmente (fino al 50% e oltre) il funzionamento dei computer quando si leggono o si scrivono dati sui dischi del sistema.

3. **Abilitare la massima protezione nel programma anti-virus** , in modo che controlli automaticamente anche i messaggi di posta elettronica (file allegati compresi) trasmessi o ricevuti.
4. **Abilitare livelli di protezione elevati nei programmi di posta elettronica, di navigazione Web, ecc.**, in modo che eventuali virus, programmi troiani, siti web untori (in grado di trasmettere virus con la sola visualizzazione di una pagina Web contenente script-virus, ecc.) non trovino le *porte aperte*.
5. **Aggiornare periodicamente il software soggetto a bachi nella sicurezza** (sistema operativo, servizi di rete, programmi di posta, di navigazione e altri ancora). In particolare si raccomanda agli utilizzatori di sistemi Windows, di attivare periodicamente (almeno 1 volte alla settimana) il comando di *Windows Update* attivabile dal menu Avvio / *Start* oppure dal programma Internet Explorer -> Strumenti -> **Windows Update** (scegliendo poi le voci *Aggiornamento prodotti* -> *Aggiornamenti critici* o sulla *Sicurezza*).
6. **Controllare periodicamente tutti i file presenti nei dischi rigidi** del proprio PC.

7. **Mettere in quarantena i file di provenienza esterna**, ovvero isolare in un direttorio dedicato i file, eseguibili e non, di cui non si è sicuri e ricontrollarli periodicamente con l'anti-virus aggiornato.
8. **Adottare delle convenzioni nello scambio di file con soggetti esterni**, ovvero:
    - specificare / comunicare in anticipo quali sono le convenzioni adottate in caso di trasmissione e attese in caso di risposta;
    - specificare la lista degli oggetti trasmessi e per ciascuno di essi una serie di riferimenti (descrizione contenuto, dimensioni, codice di controllo, ecc.).
9. **Nei sistemi windows, controllare i collegamenti e le icone**, ovvero assicurarsi che non cambino arbitrariamente dopo accessi esterni a internet o altro.
10. **Proteggere i pc dagli accessi esterni**, ovvero non consentire a chiunque di accedere facilmente alle risorse del PC; i metodi sono:
    - Rispettare le Regole dell'AllegatoB;
    - disabilitare i servizi di rete non usati o non protetti;
    - se possibile mantenere una traccia in file di log, ecc. degli accessi esterni per eventuali controlli periodici.

Mantenere aggiornata la descrizione delle protezioni adottate in luoghi a loro volta protetti (non nello stesso PC).

11. **Non fidarsi ciecamente del programma anti-virus** in quanto:
    - ci sono almeno *tre periodi di latenza* durante i quali non si può fare affidamento sulla sua protezione:
        1. il virus si diffonde ma non è riconosciuto come tale;
        2. il virus è riconosciuto come tale ma non è disponibile l'*antidoto;*
        3. l'antidoto è disponibile ma gli utenti non hanno ancora aggiornato il programma anti-virus oppure non hanno attivato una ricerca estesa in tutti i supporti (dischi rigidi, dischetti, CD, ecc.) ove si può annidare;
    - i programmi non sono mai perfetti al 100% e possono non riconoscere sempre tutte le forme in cui si presenta un virus;
    - non si può escludere che in futuro i virus attacchino o disabilitino proprio i programmi anti-virus.

In caso di dubbi è meglio essere prudenti, affidarsi al buon senso, chiedere all'amministratore di sistema ed eventualmente cercare notizie aggiornate su internet.

Linee guida per la sicurezza

Decalogo

1. UTILIZZARE LE CHIAVI

Il primo livello di protezione di qualunque sistema è quello fisico; è vero che una porta chiusa può in molti casi non costituire una protezione sufficiente, ma è anche vero che pone se non altro un primo ostacolo, e richiede comunque uno sforzo volontario non banale per la sua rimozione. È fin troppo facile per un estraneo entrare in un ufficio non chiuso a chiave e sbirciare i documenti posti su una scrivania; pertanto, chiudete a chiave il vostro ufficio alla fine della giornata e chiudete i documenti a chiave nei cassetti ogni volta che potete.

2. CONSERVATE I DISCHETTI IN UN LUOGO SICURO

Per i dischetti si applicano gli stessi criteri che per i documenti cartacei, con l'ulteriore pericolo che il loro smarrimento (che può anche essere dovuto a un furto) può passare più facilmente inosservato. A meno che non siate sicuri che contengano solo informazioni non sensibili, riponeteli sotto chiave. In alternativa i moderni sistemi di messaggistica consentono lo scambio di file in modo più pratico che non usando un floppy.

Quando rimuovete un file, i dati non vengono effettivamente cancellati ma soltanto marcati come non utilizzati, e sono facilmente recuperabili. Neanche la formattazione assicura l'eliminazione dei dati; solo l'utilizzo di un programma apposito garantisce che sul dischetto non resti traccia dei dati precedenti. Nel dubbio, è sempre meglio usare un dischetto nuovo.

3. USO DELLE PASSWORD

Vi sono diverse categorie di password, ognuna con il proprio ruolo preciso:

a) **password di BIOS:** La password di accesso al computer impedisce l'utilizzo improprio della postazione.
b) **password di rete:** La password di accesso alla rete impedisce che l'eventuale accesso non autorizzato a una postazione renda disponibili tutte le risorse dell'Ufficio/Ente.
c) **password di procedura:** La password dei programmi specifici permette di restringere l'accesso ai dati al solo personale autorizzato.
d) **password di screen saver:** La password del salva-schermo impedisce che una assenza momentanea permetta ad una persona non autorizzata di utilizzare il pc.

Imparate a utilizzare questi quattro tipi fondamentali di password, e mantenete distinta dalle altre almeno quella di tipo *a)*, che può dover essere resa nota, almeno temporaneamente, ai tecnici incaricati dell'assistenza.

4. GESTIONE E CUSTODIA DELLE PASSWORD

Anche se molti programmi non ripetono in chiaro la password sullo schermo, quando digitate la vostra password, questa potrebbe essere letta guardando i tasti che state battendo, anche se avete buone capacità di dattiloscrittura.
Non scrivete la vostra password, meno che mai vicino alla vostra postazione di lavoro. L'unico affidabile dispositivo di registrazione è la vostra memoria. Se avete necessità di conservare traccia delle password per scritto, non lasciate in giro i fogli utilizzati

5. USO DEL VOSTRO COMPUTER DA PARTE DI PERSONALE ESTERNO

Assicuratevi dell'identità della persona e delle autorizzazioni ad operare da parte di personale esterno se ha bisogno di installare del nuovo software/hardware sul vostro computer.

6. NON INSTALLATE PROGRAMMI NON AUTORIZZATI

Solo i programmi istituzionali o acquistati dall'Amministrazione con regolare licenza sono autorizzati. Se il vostro lavoro richiede l'utilizzo di programmi specifici, consultatevi con il responsabile del trattamento dati.

7. NON UTILIZZATE APPARECCHI NON AUTORIZZATI

L'utilizzo di modem su postazioni di lavoro collegati alla rete offre una porta d'accesso dall'esterno non solo al vostro computer, ma a tutta la rete, ed è quindi vietata. Per l'utilizzo di altri apparecchi, consultatevi con il responsabile del trattamento dati del vostro ufficio o con l'Amministratore di sistema.

8. APPLICATE CON CURA LE LINEE GUIDA RELATIVE AI VIRUS

La prevenzione dalle infezioni da virus sul vostro computer è molto più facile e comporta uno spreco di tempo molto minore della correzione degli effetti di un virus; tra l'altro, potreste incorrere in una perdita irreparabile di dati.

9. CONTROLLATE LA POLITICA LOCALE RELATIVA AI BACKUP

I vostri dati potrebbero essere gestiti da un *file server*, oppure essere gestiti in locale e trasferiti in un server solo al momento del backup. Verificate con il personale locale la situazione.

10. ATTENZIONE ALLE STAMPE DI DOCUMENTI RISERVATI

Non lasciate accedere alle stampe persone non autorizzate; se la stampante non si trova sulla vostra scrivania recatevi quanto prima a ritirare le stampe. Distruggete personalmente le stampe quando non servono più o quando vengono create copie inutili.

Come inviare messaggi con file allegati

Nell'inviare messaggi di posta elettronica si corrono i seguenti rischi:

- rischio di inviare file infetti (documenti Word, ecc.);
- rischio che un virus modifichi i file o cerchi di aggiungere un file estraneo nella fase di trasmissione del messaggio (nel caso in cui il programma di posta sia infettato);
- rischio che un virus modifichi i file quando il destinatario li riceve.

L'obiettivo è quindi quello di inviare sempre e comunque le seguenti informazioni inserite alla fine del testo principale del messaggio:

- numero di file allegati;
- eventualmente per ogni file allegato:
  - nome file;
  - breve descrizione contenuto (1 riga);

Se non ci sono file allegati, si precisa: N. 0 file allegati.

Si noti che queste informazioni sono volutamente ridondanti dato che dovrebbero coincidere con quelle fornite dai programmi di posta con l'opzione *proprietà* relative al messaggio o ai file allegati.

Comprimere in archivi ZIP i file allegati

Comprimere i file allegati in un unico archivio con i programmi relativi (zip, tar, ecc.) apporta i seguenti vantaggi:

- riduce di 10-15 volte le dimensioni dei documenti e di 3-4 volte le dimensioni dei programmi eseguibili (*.exe, ecc.);
- la congruenza dei dati compressi e archiviati è garantita da codici di controllo propri dei programmi di compressione quindi qualsiasi corruzione ad opera di virus rende inservibile l'archivio stesso.

Ovviamente resta la possibilità che un virus sia tanto intelligente da decomprimere un file archivio, inserire le sue modifiche e poi ricomprimere l'archivio; per questo dovrebbe essere mantenuta la sopraccitata lista di descrizione dei file allegati.

Inviare i documenti in formati sicuri e portabili

Dato che nei file di Word, Excel, PowerPoint si possono annidare virus di macro, è opportuno, almeno per i documenti di testo Word (*.doc), usare i seguenti formati alternativi:

RTF (*.rtf)

Rich Text Format, è compatibile con quasi tutti i programmi di elaborazione testi sulla maggioranza dei sistemi operativi (Windows, DOS, OS/2, MacIntosh, Unix, ecc.); ha il piccolo difetto che le dimensioni dei file tendono ad essere parecchio maggiori rispetto agli originali (la compressione esterna elimina questo svantaggio).

XML (*.xml, *.html)

Extensible MarkUp Language, formato con marcatori simili a quelli dell'HTML, è uno standard che può essere creato/letto solo con programmi recenti (es. Office 2000).

PDF (*.pdf)
Portable Document Format, necessita di un apposito programma per essere creato, ma i lettori PDF sono molto diffusi (es. *Acrobat Reader*); utile se il destinatario non deve modificare il contenuto del file.

Come trattare i file allegati ricevuti con i messaggi di posta

La ricezione della posta elettronica richiede ovviamente qualche precauzione in più rispetto alla spedizione.

Attivare l'anti-virus

Prima di ricevere nuova posta elettronica è opportuno attivare il programma anti-virus in modo che questo cerchi di intercettare eventuali file infetti (l'anti-virus esamina anche i file compressi in archivi ZIP).

Non visualizzare, né eseguire eventuali file allegati

Se ci sono file allegati procedere come segue.

1. **Non** *aprire* per nessuna ragione i file allegati direttamente dal programma di posta elettronica (evitare perfino la pre-visualizzazione/anteprima dei contenuti).
2. **Salvare su disco rigido** (in un apposito direttorio) i file allegati (mantenendo i nomi originali o rinominandoli con l'opzione "Salva con nome"); questa azione dovrebbe consentire a qualsiasi programma anti-virus di esaminare il contenuto del file salvato e quindi di intercettare eventuali virus.
3. **Prima di aprire i file allegati salvati**, eseguire le seguenti azioni:
    1. confrontare i nomi ricevuti, le dimensioni dei file, ecc. con le relative informazioni contenute nell'apposita lista descrittiva del messaggio;
    2. se la lista descrittiva manca o non si è assolutamente sicuri che i file ricevuti siano corretti, **si consiglia di contattare il mittente** per ottenere le necessarie informazioni;
4. **Periodicamente ricontrollare** i **vecchi file allegati** salvati su disco rigido per accertarsi, a distanza di tempo e con l'anti-virus aggiornato, della reale assenza di virus.

Come prevenire i virus

USATE SOLTANTO PROGRAMMI PROVENIENTI DA FONTI FIDATE

Copie sospette di programmi possono contenere virus o altro software dannoso. Ogni programma e/o file deve essere sottoposto alla scansione prima di essere installato. Non utilizzate programmi non autorizzati, con particolare riferimento ai videogiochi che sono spesso utilizzati per veicolare virus.

PROTEGGETE I VOSTRI DISCHETTI DA SCRITTURA QUANDO POSSIBILE

In questo modo eviterete le scritture accidentali, magari tentate da un virus che sta cercando di propagarsi. I virus non possono in ogni caso aggirare la protezione meccanica (nel dubbio non utilizzare floppy ma la posta elettronica per lo scambio di documenti inferiori a 1,4 mb).

ASSICURATEVI CHE IL VOSTRO SOFTWARE ANTIVIRUS SIA AGGIORNATO

La tempestività nell'azione di bonifica è essenziale per limitare i danni che un virus può causare; inoltre è vitale che il programma antivirus conosca gli ultimi aggiornamenti sulle "impronte virali" dei nuovi virus.

"Disciplinare tecnico in materia di misure minime di sicurezza" (artt. da 33 a 36 del Codice sulla privacy).

Sotto al titolo della regola è riportato in corsivo il testo originale così come scritto nell'Allegato B.

Regola 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.

Nome utente e password sono strettamente personali; l'utente è tenuto a non comunicarle ad altri.

Cosa NON fare:

- NON dite a nessuno la vostra password; ricordate che lo scopo principale per cui usate una password è assicurare che nessun altro possa utilizzare le vostre risorse o possa farlo a vostro nome
- NON scrivete la password da nessuna parte che possa essere letta facilmente, soprattutto vicino al computer
- Quando immettete la password NON fate sbirciare a nessuno quello che state battendo sulla tastiera; il più semplice metodo per l'accesso illecito a un sistema consiste nell'indovinare la password dell'utente legittimo.
- NON usate il vostro nome utente: è la password più semplice da indovinare
- NON usate password che possano in qualche modo essere legate a voi come, ad esempio, il vostro nome, quello di vostra moglie/marito, dei figli, del cane, date di nascita, numeri di telefono ecc.

Cosa fare

- Cambiare la password a intervalli regolari. Chiedete all'amministratore di sistema quali sono le sue raccomandazioni sulla frequenza del cambio; a seconda del tipo di sistema l'intervallo raccomandato per il cambio può andare da tre fino a 12 mesi
- Usare password lunghe almeno 8 caratteri con un misto di lettere, numeri e segni di interpunzione
- Scegliere la password di accensione diversa dalle altre password

Regola 9

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

Durante una normale sessione di lavoro l'utente che si allontana dal pc è obbligato ad utilizzare l'utilità di *salva schermo con password* per evitare l'uso non autorizzato del pc da parte di altri utenti.

Per attivare il salva schermo accedere all'utility "Schermo" da Avvio/Start - Impostazioni - Pannello di controllo. Cliccare sulla scheda "Screen saver" e dall'elenco a discesa scegliere un tipo di screen saver (salva schermo); dopodichè impostare il tempo di attesa (preferibilmente basso) ed attivare la protezione.

Ogniqualvolta il pc rimarrà inattivo per il periodo di tempo scelto, verrà visualizzato il salva schermo e sarò richiesto l'inserimento della password prima di ri-accedere al pc.

Senza dover attendere il trascorrere del tempo di inattività, il pc può essere bloccato utilizzando la combinazione di tasti CTRL+ALT+Canc seguita dal tasto Invio.

Regola 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.

Tutte le password sono custodite singolarmente in busta chiusa dall'amministratore del sistema.

Qualora si ritenga necessario rendere disponibile una risorsa dati momentaneamente non accessibile per assenza o impedimento dell'incaricato, l'amministratore di sistema, su incarico del titolare, provvede all'apertura della busta contenente le password relative e inserisce i dati sul pc.

Conclusa la sessione di lavoro è compito dell'amministratore sostituire le credenziali con nuovi dati da comunicare all'interessato.

Regola 18

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Deve essere garantito il salvataggio dei dati con frequenza giornaliera. L'amministratore di sistema, anche in collaborazione con consulenti esterni all'Ente, provvede a impostare il salvataggio dei dati in modalità automatica.

È compito dell'amministratore di sistema, o suo incaricato, sostituire il supporto di back-up quotidianamente .

È compito dell'amministratore di sistema, o suo incaricato, consultare il file di log relativo all'ultimo salvataggio effettuato per verificare l'eventuale presenza di errori.

L'amministratore di sistema in accordo coi vari Responsabili redige l'elenco delle banche dati da salvaguardare. Sul Documento programmatico sulla sicurezza sono inserite le banche dati attualmente in uso e l'attuale frequenza e periodicità di salvataggio.

Regola 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

I supporti removibili utilizzati per il back-up devono essere conservate in un locale diverso da quello adibito a sala server. I supporti removibili utilizzati per il back-up sono conservati in un armadio o cassettiera chiusi a chiave: l'accesso a tali supporti è consentito esclusivamente all'amministratore del sistema o suo incaricato.

Regola 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 seriori a sette giorni.

Per garantire il ripristino dei dati, l'amministratore di sistema verifica periodicamente, con cadenza almeno mensile, il contenuto dei supporti removibili utilizzati per il back-up.

Ad ulteriore garanzia deve essere monitorato, a cura dell'amministratore di sistema, lo stato di usura delle cassette e deve esserne prevista la sostituzione immediata.

Nel caso si verifichi il danneggiamento dei supporti o degli strumenti elettronici che li ospitano, è garantito che il ripristino viene effettuato entro i 2 giorni lavorativi successivi.

Regola 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.

- I fascicoli cartacei, nelle fasi di trasporto all'interno dell'ufficio, non devono permanere nei corridoi o in luoghi *non sicuri*.
- Gli incaricati devono avere accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati.
- Nessuno può accedere all'archivio se non autorizzato.

- I fascicoli se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate.
- Nel caso in cui i documenti o l'archivio contengano dati sensibili:
  a. Gli atti e i documenti contenenti i dati se affidati agli incaricati del trattamento, devono essere conservati, fino alla restituzione, in contenitori muniti di serratura, *sottochiave;*
  b. L'accesso all'archivio deve essere controllato e devono essere identificati e registrati i soggetti che vi sono ammessi dopo l'orario di chiusura dell'archivio stesso o degli uffici (regola 29);

I documenti cartacei contenenti riproduzione d'informazioni relative al trattamento devono essere conservati e custoditi con le modalità suddette.

AGGIORNAMENTO ANNUALE DEL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

- RELAZIONE ACCOMPAGNATORIA -

L'art. 19 – allegato B del D.Lgs. 196/2003 prevede l'obbligo di aggiornamento del Documento Programmatico sulla Sicurezza (DPS) entro il 31 marzo di ogni anno.
Il Comune di Fossalta di Piave ha adottato per la prima volta tale documento con deliberazione di Giunta Comunale n. 36 del 28/03/2000. Successivamente, in base alle novità introdotte dalla suddetta normativa e dal relativo regolamento, è stato predisposto il nuovo D.P.S. con deliberazione di Giunta Comunale n. 149 del 28/12/2006. In data 31/03/2010 è stato approvato l'ultimo aggiornamento del DPS, così come imposto dalla vigente normativa, con deliberazione di Giunta Comunale n. 41.
Rispetto all'ultimo aggiornamento vi sono alcune modifiche da apportare, anche se vi sono interventi ancora in itinere o in attesa di valutazione, visto il considerevole onere economico che comportano.

Soggetti coinvolti

Per quanto riguarda i soggetti autorizzati al trattamento dei dati, l'unica rilevante novità è rappresentata dall'istituizione l'Area Polizia Locale a seguito dell'approvazione della convenzione per la gestione associata e coordinata del servizio di Polizia Locale con i Comuni di Quarto d'Altino, Meolo, Roncade e Silea. Si è reso necessario un aggiornamento del Regolamento degli uffici e dei servizi approvato con deliberazione della Giunta Comunale n. 8 del 26/01/2011, dal quale si rileva che l'assetto organizzativo, anche in materia di trattamento dati è il seguente:

Area	Titolare	Responsabile	Incaricati
Amministrativa	☑	☑	☑
Tecnica		☑	☐
Direzionale		☑	☑
Polizia Locale		☑	☑

Come si può notare dalla tabella, non è ancora stata formalizzata la nomina degli incaricati dell'Area Tecnica. Per quanto riguarda le altre Aree sono stati regolarmente individuati tutti gli incaricati al trattamento dei dati e, sebbene vi siano stati degli avvicendamenti riguardanti i Responsabili di Area, tali nomine sono da ritenersi interamente confermate, poiché non vi sono state modifiche alle attribuzioni dei singoli incaricati al trattamento dei dati.

Elementi di rischio

Con particolare riferimento alla scheda n. 6 "Elementi di rischio" del DPS, sono stati effettuati i seguenti interventi:

- è stato acquistato un nuovo server, in quanto quello esistente non era più in grado di far fronte alle ordinarie necessità dell'Ente, soprattutto in termini di spazio disponibile. Inoltre il "vecchio" server risultava tecnologicamente inadeguato;
- è stato aggiornato l'antivirus installato sul server;
- è stato sostituito il firewall per l'accesso a internet con uno più recente;
- è stato aggiornato il software antispam;
- è stato acquistato un gruppo di continuità a servizio del server, per evitare problemi connessi all'interruzione improvvisa di energia elettrica o a cali di tensione che si verificano piuttosto di frequente nella rete elettrica;

- è stato acquistato un armadio contenitore per contenere il server e i relativi accessori. Tale attrezzatura è dotata di serrature e consente di racchiudere le strumentazioni informatiche in modo più razionale e sicuro evitando soprattutto il distacco accidentale di cavi e connessioni che prima si presentavano in modo disordinato e confuso.

Per quanto riguarda i sistemi antincendio sono stati terminati i lavori di adeguamento della sede municipale alla normativa di prevenzione incendi, che prevede l'installazione di un impianto nella zona adibita ad archivi situata nel seminterrato. Il progetto in questione prevedeva l'installazione di rilevatori di fumo e la realizzazione di un impianto di estinzione a gas. Al momento si attende il rilascio del Certificato di Prevenzione Incendi da parte dei Vigili del Fuoco.

Interventi formativi

Il personale, ed in particolare i responsabili del trattamento, sono stati adeguatamente informati sui vari obblighi ed adempimenti. Ad ognuno sono state consegnate delle dispense che riassumono le principali responsabilità e le norme di comportamento. In occasione dei periodici aggiornamenti del Documento Programmatico sulla Sicurezza, si provvede comunque a trasmettere copia dei provvedimenti ai Responsabili di Servizio in quanto Responsabili del trattamento dei dati. Si ritiene tuttavia opportuno aggiornare periodicamente il personale interessato, soprattutto in caso di modifiche alla normativa.

Fossalta di Piave, 18 aprile 2011