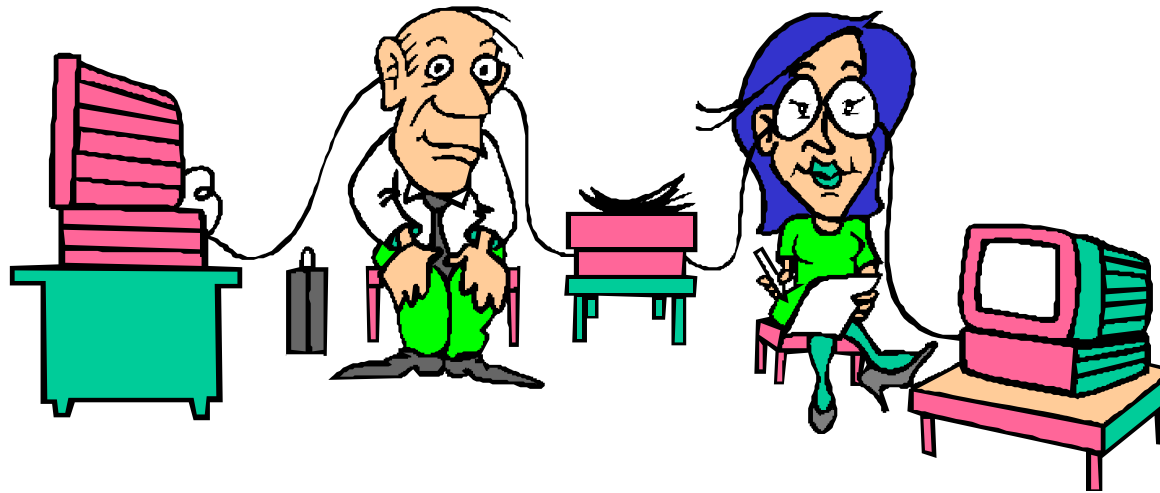


ISIS "C.A. Dalla Chiesa" a.s. 2011-2012



Privacy

Prof. Pier Giorgio Galli
Montefiascone 19/09/2011

Perché siamo qui

Codice in materia di protezione dei dati personali:
Decreto legislativo 30/06/2003, n. 196

Art. 4. Definizioni

“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, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;



Trattamento dei dati cartacei



Trattamento dei dati elettronici

Tipi di dato

Art. 4. Definizioni

“**dato personale**”, 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; [**i voti, i giudizi sono dati personali**]

“**dati identificativi**”, i dati personali che permettono l'identificazione diretta dell'interessato;

“**dati sensibili**”, i dati personali idonei a rivelare l'origine 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 [**i certificati medici, i verbali H sono dati sensibili**];

“**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 d.P.R. 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;

Titolare

Art. 28. Titolare del trattamento

Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Nella scuola **titolare del trattamento è l'Istituzione Scolastica legalmente rappresentata pro tempore dal Dirigente Scolastico.**

Responsabile

Art. 29. Responsabile del trattamento

1. Il responsabile è designato dal titolare **facoltativamente**.
2. Se designato, il responsabile **è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.**
3. Ove necessario per esigenze organizzative, **possono essere designati responsabili più soggetti**, anche mediante suddivisione di compiti.
4. I compiti affidati al responsabile **sono analiticamente specificati** per iscritto dal titolare.
5. Il responsabile effettua il trattamento **attenendosi alle istruzioni impartite dal titolare** il quale, anche tramite verifiche periodiche, **vigila** sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Incaricato

Art. 30. Incaricati del trattamento

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano **sotto la diretta autorità del titolare** o del responsabile, attenendosi alle **istruzioni impartite**¹.
2. La **designazione** è effettuata per iscritto e individua puntualmente **l'ambito** del trattamento consentito. ... continua ...

¹ Il codice di realtà impone all'incaricato di attenersi alle istruzioni che gli vengono impartite, presupponendo peraltro un correlato obbligo per il titolare ed il responsabile sotto la cui diretta autorità egli opera di istruirlo.

G. Cassano, S.Fadda, "Commento al testo unico sulla privacy", IPSOA, 2004.

Regole (ulteriori) per i soggetti pubblici

Art. 18. c. 2

Qualunque trattamento di **dati personali** da parte di soggetti pubblici è consentito soltanto per lo **svolgimento delle funzioni istituzionali** *[se **diversi da sensibili o giudiziari** è consentito anche in mancanza di una norma di legge o di regolamento che lo prevede espressamente (art. 19 c.1)].*

Art. 20. c. 1

Il trattamento dei **dati sensibili** da parte di soggetti pubblici è consentito **solo se autorizzato da espressa disposizione di legge** *[o, per le scuole, con regolamento]* **nella quale sono specificati i tipi di dati che possono essere trattati** e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

Art. 21

Analogo al precedente per i **dati giudiziari**.

DM 305/2006 - Regolamento

Art. 1 - Oggetto del regolamento

Il presente regolamento, in attuazione [..omissis..] **identifica nelle [sette] schede allegate**, che ne formano parte integrante, le tipologie di dati sensibili e giudiziarie di operazioni indispensabili **per la gestione del sistema dell'istruzione, nel perseguimento delle finalita' di rilevante interesse pubblico individuate..**

Art. 2 c. 1 - Individuazione dei dati

I dati sensibili e giudiziari individuati dal presente regolamento sono trattati previa verifica della loro pertinenza, completezza e **indispensabilita'** rispetto alle finalita' perseguite nei singoli casi, specie quando la raccolta non avvenga presso l'interessato.

Misure di sicurezza

Art. 31. Obblighi di sicurezza

I dati personali oggetto di trattamento sono custoditi e controllati, **anche in relazione alle conoscenze acquisite in base al progresso tecnico**, alla **natura dei dati** e alle specifiche caratteristiche del trattamento, **in modo da ridurre al minimo**, mediante l'adozione di idonee e preventive misure di sicurezza, **i rischi di distruzione o perdita**, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Determina la responsabilità, con relativo risarcimento, di **tipo civile**
[Art 15. **Chiunque** cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi (...)]

Misure minime

Art. 34. Misure minime

Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o (...) volte ad assicurare **un livello minimo** di protezione dei dati personali.

Determina la responsabilità di **tipo penale**

Art. 169. Misure di sicurezza

1. **Chiunque** *[titolare, responsabile o incaricato]*, essendovi tenuto, **omette** di adottare le misure minime previste dall'articolo 33 è punito con.....

Misure minime: sanzioni

... l'arresto sino a due anni.

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, **se risulta l'adempimento alla prescrizione**, l'autore del reato è ammesso dal Garante a pagare una somma **pari al quarto del massimo** della sanzione stabilita per la violazione amministrativa.
L'adempimento e il pagamento estinguono il reato (...)

P.S. massimo della sanzione € 120.000

Trattamenti senza l'ausilio di strumenti elettronici

Art. 35

Trattamento senza strumenti elettronici **misure minime**:

- a) Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati *[in pratica la designazione annuale]*.
- b) Previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati *[che vedremo più avanti nei dettagli]*.
- c) Previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina di accesso finalizzata all'isntificazione degli incaricati *[non interessano i docenti]*.

Trattamenti con strumenti elettronici

Art. 34.

1. Il trattamento di dati personali effettuato con strumenti elettronici è **consentito solo se sono adottate**, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti **misure minime**:
 - **autenticazione informatica;**
 - **adozione di una procedura di gestione delle credenziali di autorizzazione;**
 - **protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;**
 - ecc. non di interesse per i docenti.

Il docente è incaricato...

... del trattamento dei dati personali, identificativi, sensibili e giudiziari degli studenti raccolti per l'espletamento della funzione docente:

- 1. nel registro di classe;**
- 2. nel registro personale del docente;**
- 3. nei registri dei verbali;**
- 4. nella raccolta degli elaborati scritti o grafici o elettronici prodotti dagli studenti;**
- 5. negli archivi elettronici personali del docente memorizzati presso l'istituzione scolastica.**

Nell'elenco non sono indicati brogliacci, appunti, agende, computer domestici, notebook, ecc., perché il Titolare del trattamento è in grado di garantire le misure minime solo presso la sede scolastica.

Designazione

Istruzioni di carattere generale I

I dati personali oggetto del trattamento sono (v. art. 11):

1. trattati in modo lecito e secondo correttezza;
2. raccolti e registrati solo per gli scopi strettamente necessari alla funzione docente ;
3. esatti e, se necessario, aggiornati;
4. pertinenti, completi e non eccedenti le finalità della funzione docente;

Istruzioni di carattere generale II

- 5) conservati e custoditi nel rispetto delle misure di sicurezza predisposte dall'Istituzione Scolastica:
- a) trattati e conservati solo ed esclusivamente presso l'Istituzione Scolastica. E' fatto esplicito divieto di far uscire i dati personali degli studenti dalla sede scolastica anche temporaneamente. **È fatta deroga per quanto attiene alle operazioni relative alla valutazione degli elaborati scritti, purché su ciascuno di essi non compaia il nome dell'alunno bensì il relativo il numero d'ordine del registro di classe;**
 - b) se cartacei mai lasciati incustoditi. Il docente dovrà sempre portarli con sé o chiuderli a chiave nel cassetto personale munito di serratura;
 - c) mai comunicati o diffusi al di fuori del Dirigente Scolastico, della classe, dei componenti degli organi collegiali di pertinenza, dei genitori (o di chi ne fa le veci);
 - d) nascosti alla vista di terzi durante il trattamento;
 - e) in assenza, anche temporanea, del docente chiusi a chiave nel cassetto personale;
 - f) se elettronici memorizzati esclusivamente nella cartella personale del docente con accesso attraverso credenziali di autenticazione.

Designazione

Istruzioni di carattere particolare I

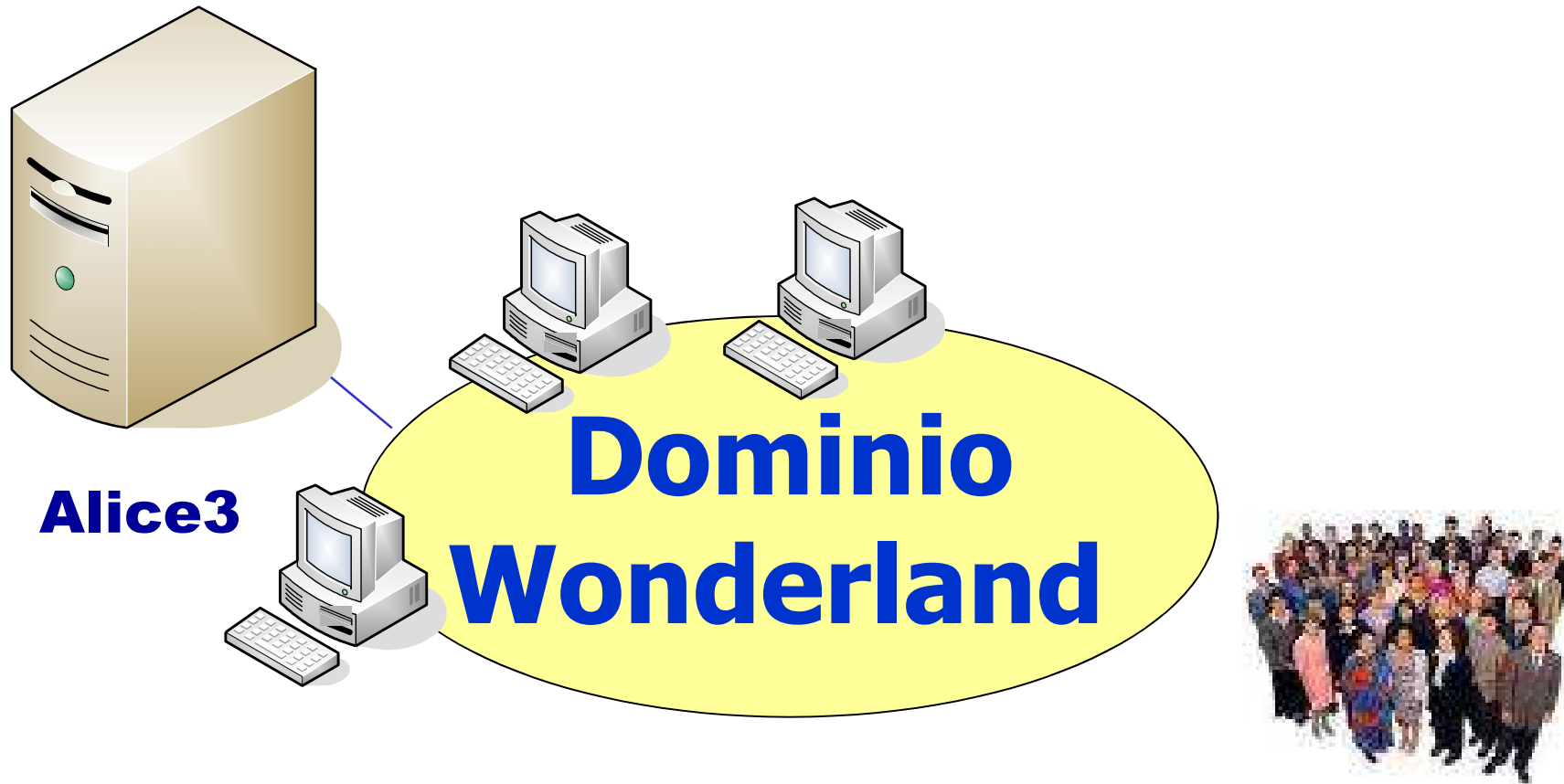
1. dovrà raccogliere i certificati medici degli studenti e, dopo averli annotati nel registro di classe, consegnarli il giorno stesso in segreteria didattica;
2. appena in classe dovrà verificare la presenza e lo stato del registro di classe. In caso di smarrimento o di danneggiamento dovrà tempestivamente darne notizia al Dirigente Scolastico;
3. dovrà consegnare le comunicazioni scritte per le famiglie in segreteria didattica che provvederà all'inoltrato. E' fatto divieto esplicito di comunicare attraverso il diario o i quaderni dello studente;
4. al termine dell'anno scolastico, o precedentemente se ritenuto opportuno, dovrà consegnare gli elaborati cartacei degli studenti in segreteria didattica;
5. al termine dell'anno scolastico, o precedentemente se ritenuto opportuno, dovrà consegnare gli elaborati elettronici consegnati dagli studenti in segreteria didattica memorizzati in un CD o DVD;
6. al termine dell'anno scolastico dovrà consegnare tutti i documenti contenenti dati personali degli studenti in segreteria didattica;

Istruzioni di carattere particolare II

7. nel caso in cui il docente provveda per la prima alla gestione dei dati attraverso il sistema informativo dell'Istituzione Scolastica, unitamente al presente ordine di servizio gli sono consegnate le credenziali di autenticazione provvisorie. Tali credenziali impongono il cambiamento della password al primo accesso secondo i criteri di complessità richiesti dal sistema di autenticazione. Da quel momento l'incaricato dovrà porre in essere tutti i comportamenti necessari al fine di salvaguardare la segretezza della password. In particolare: **non dovrà rivelarla, di propria iniziativa o dietro richiesta, ad alcuno; dovrà custodirla in modo da non renderla facilmente accessibile a terzi.** E' inoltre necessario evitare di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati.
8. segnalare al titolare o al responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
9. dovrà porre in atto tempestivamente tutte le rimanenti azioni che di volta in volta si rendano necessarie affinché il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali stessi.

Organizzazione generale

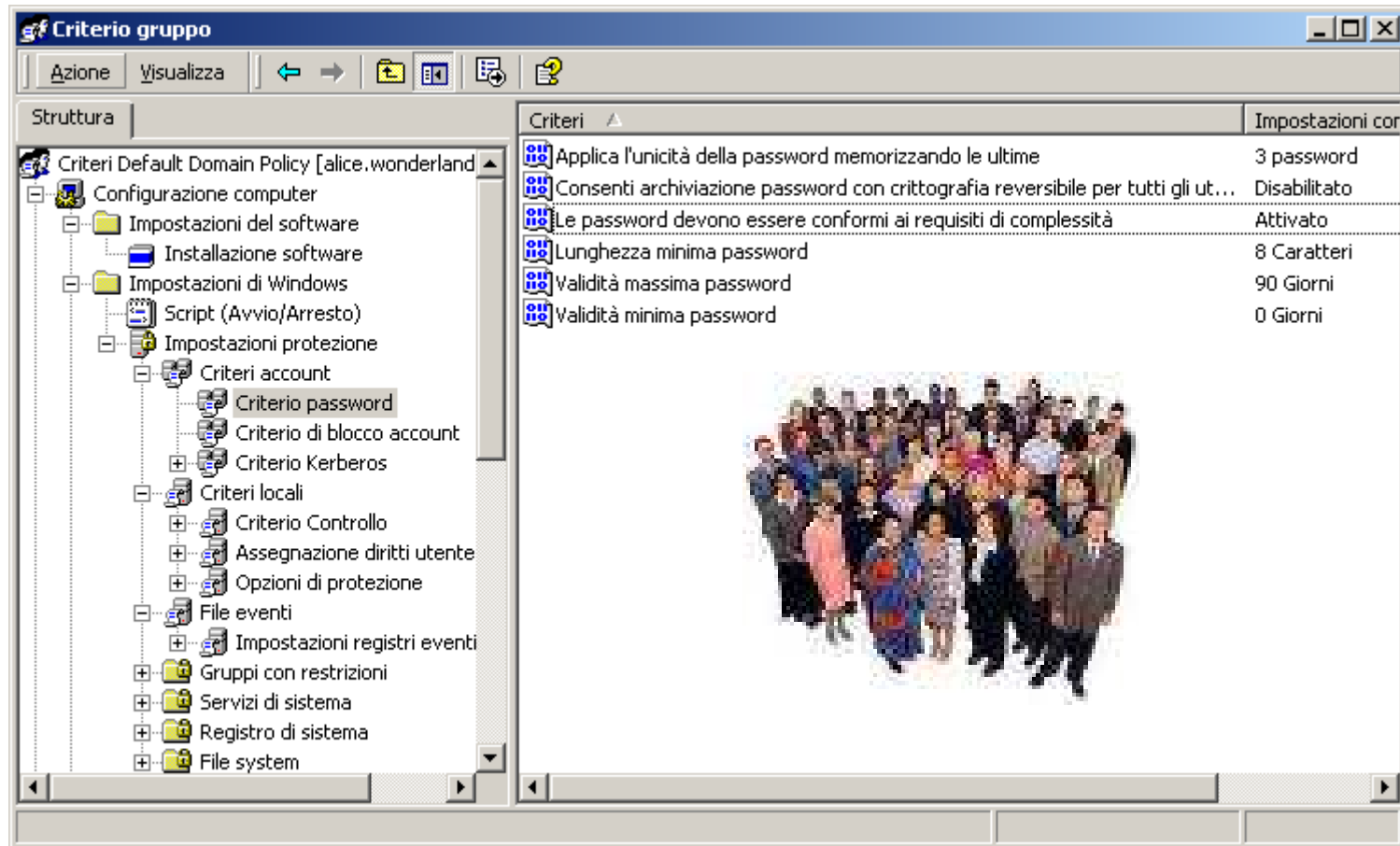
- I verbali dei consigli di classe sono conservati nella presidenza della sede in Via Aldo Moro nella diretta custodia del Titolare.
- Nella sala professori non dovranno essere presenti i dati personali degli alunni se non all'interno dei cassettei dei professori.
- La posta elettronica vtis00900l@istruzione.it e liceo@dallachiesa.it sarà scaricata dagli addetti di segreteria;
- Tutte le circolari saranno reperibili nel sito web della scuola www.dallachiesa.it. La segreteria amministrativa provverà ad estrarne copia cartacea da collazionare in sala professori.



E' il controller di dominio che autentica l'utenza e impone al computer locale le autorizzazioni

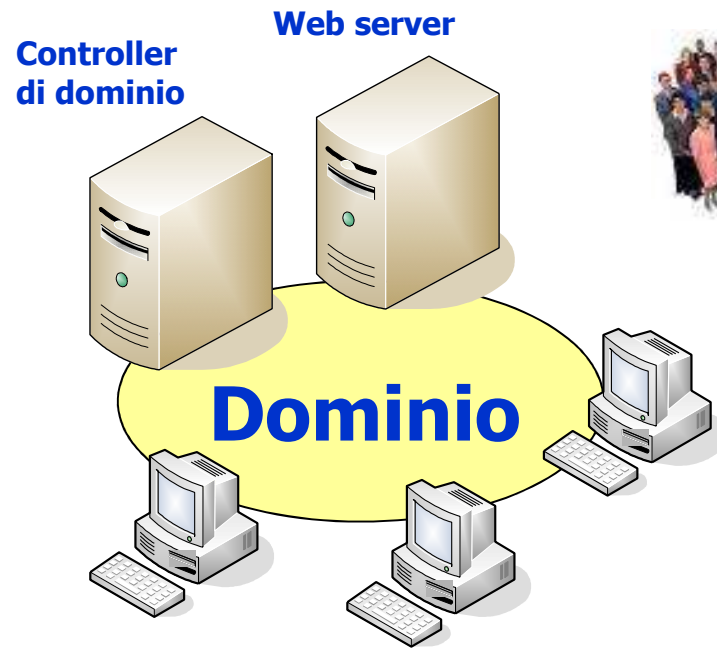


Le policy



E' il controller di dominio che impone il rinnovo della password al primo accesso e ogni tre mesi, stabilisce i criteri di complessità e...

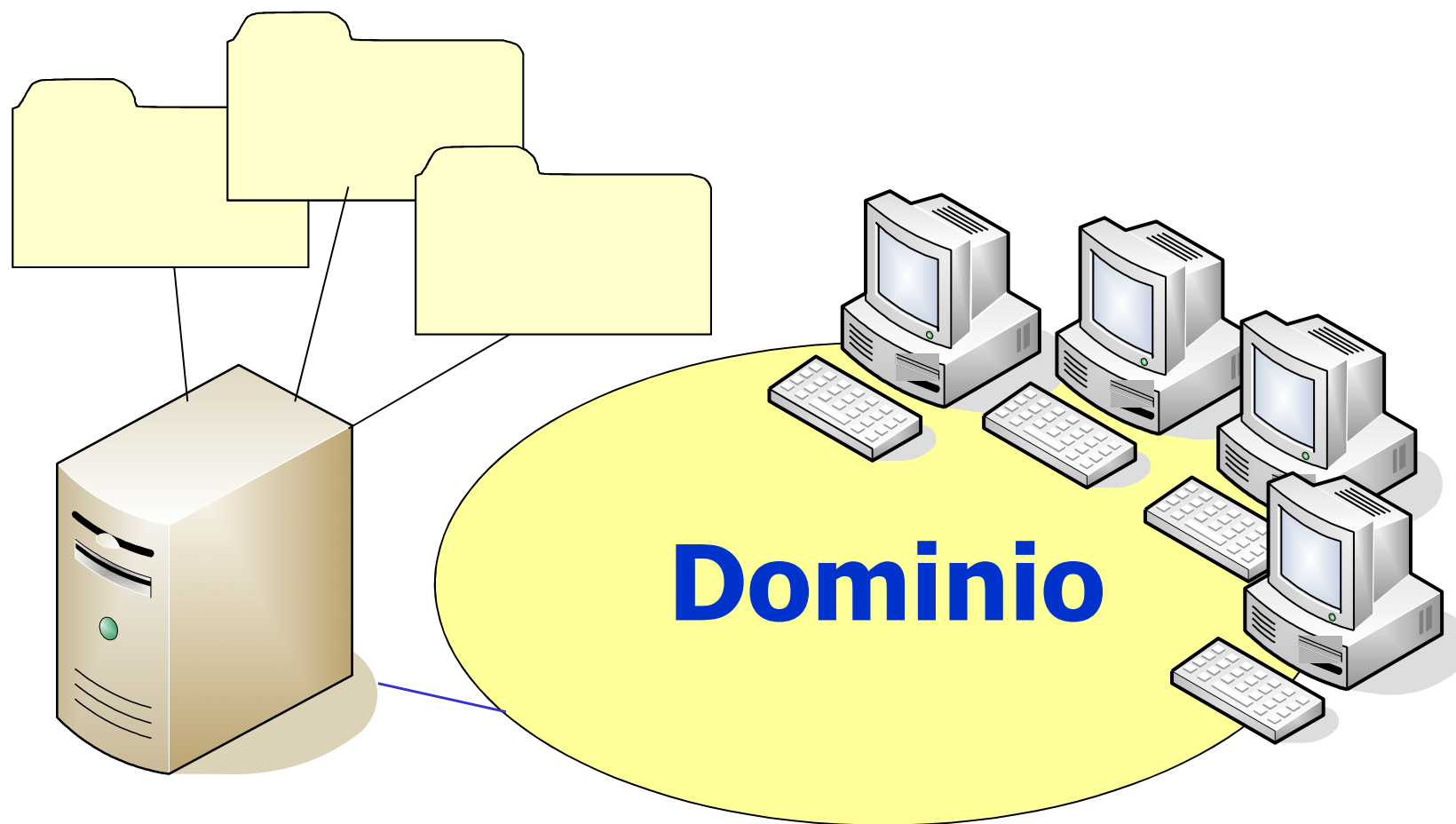
Sistema di autorizzazione



Policy di dominio:

- **accesso alle cartelle**
- **esecuzione di programmi**
- **installazione programmi**
- **accesso a internet**
- **ecc. ecc.**

Gli Archivi condivisi



Ogni incaricato accede alle cartelle di pertinenza

Protezione da virus ecc.

Art. 34. Trattamento con strumenti elettronici

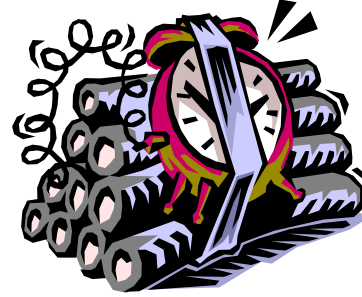
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;

Allegato B)

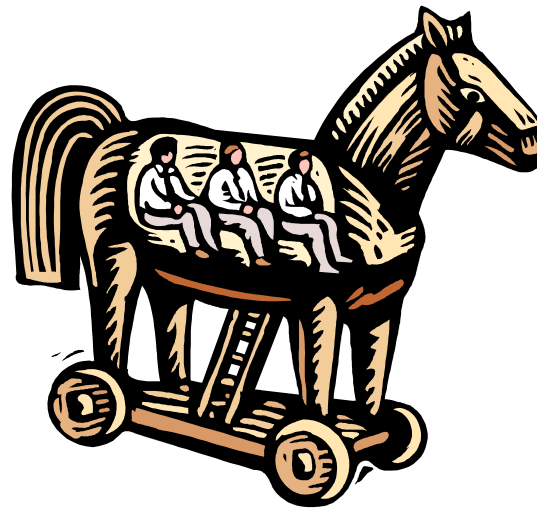
16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale [virus, malware], mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

Malware (malicious software)

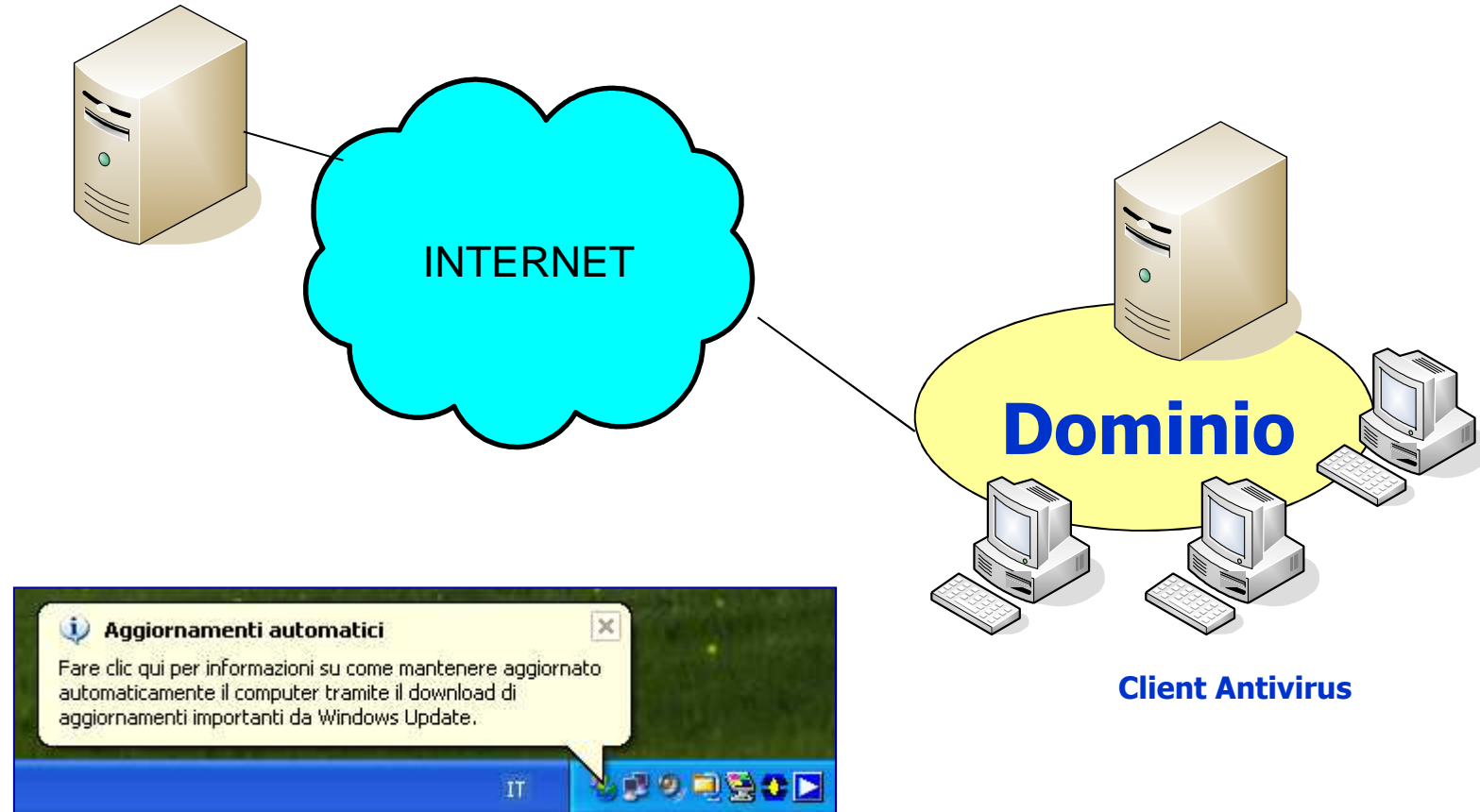


- Hoax
- Virus & Worm *(possono aprire backdoor attraverso Trojan horse o sfruttando vulnerabilità del sistema)*
- Dialer
- Spyware



Software update services

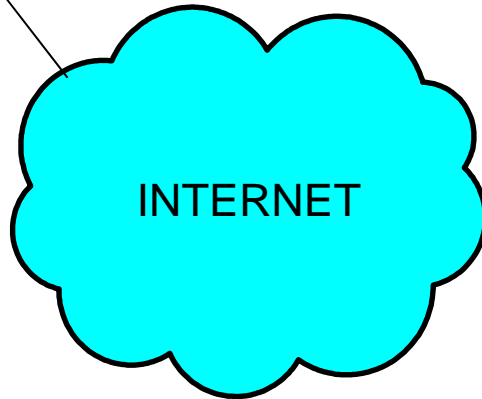
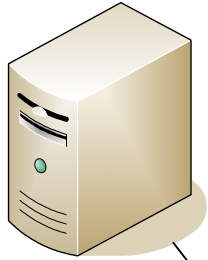
Server microsoft per la distribuzione degli aggiornamenti, patch, service pack



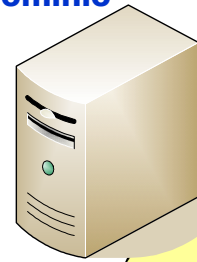
Architettura client server / multilivello

Antivirus

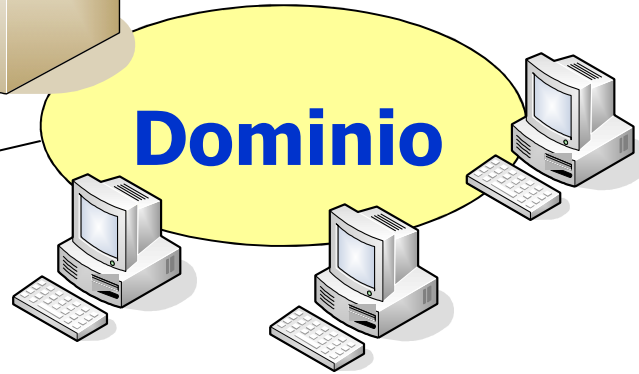
Server di distribuzione
delle definizioni



Controller
di dominio

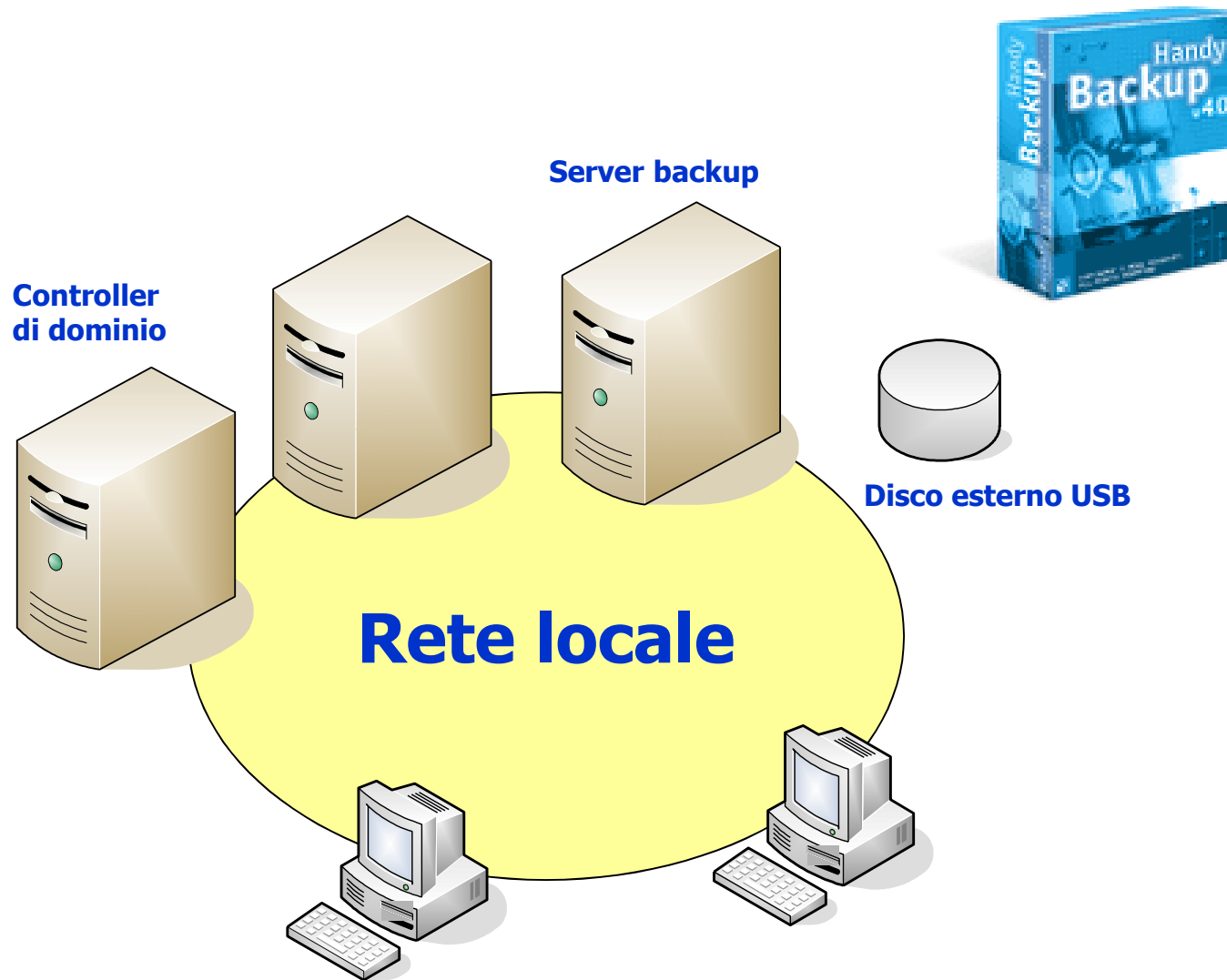


Dominio



Client Antivirus

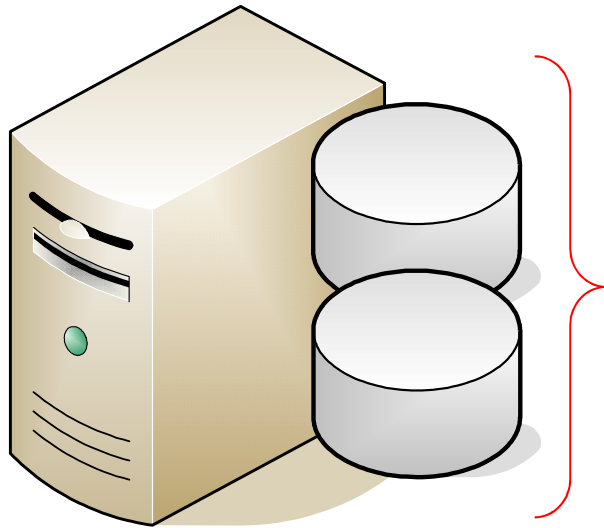
Agenti software di backup



Disaster recovery

- Calamità naturali
- Incendio
- **Furto**
- **Rottura dell'hard disk**

Windows 2003 server



- Sistemi fault tolerant
- Sistemi completamente ridondati
- armadi ignifughi
- ecc.

Dischi mirrorati

DPS

Art. 34. Trattamento con strumenti elettronici

g) tenuta di un aggiornato documento programmatico sulla sicurezza;

Sintesi - Allegato B)

Il titolare di un trattamento **di dati sensibili o di dati giudiziari** redige **anche attraverso il responsabile**, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali e la **distribuzione dei compiti e delle responsabilità; i criteri di cifratura**
- l'analisi dei rischi che incombono sui dati; le misure da adottare per garantire l'integrità e la disponibilità dei dati; la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento;
- il titolare **riferisce nella relazione del bilancio d'esercizio** dell'avvenuta redazione del DPS