

## SISTEMI OPERATIVI OBSOLETI

Come indicato da Microsoft sul proprio sito Web vi sono alcuni Sistemi Operativi non più supportati, per i quali cioè non vengono più rilasciati **aggiornamenti relativi alla protezione**. Tali informazioni vengono riassunte nella tabella che segue:

### Versioni e lingue supportate

Versione del sistema operativo	Supportato da Windows Update
<b>Windows Server 2003</b>	
<ul style="list-style-type: none"> <li>Windows Server 2003 con Service Pack 1</li> </ul>	<ul style="list-style-type: none"> <li>Attualmente supportato</li> </ul>
<ul style="list-style-type: none"> <li>Windows Server 2003</li> </ul>	<ul style="list-style-type: none"> <li>Nuovi aggiornamenti disponibili solo fino al mese di giugno 2007</li> </ul>
<b>Windows XP</b>	
<ul style="list-style-type: none"> <li>Windows XP con Service Pack 2</li> </ul>	<ul style="list-style-type: none"> <li>Attualmente supportato</li> </ul>
<ul style="list-style-type: none"> <li>Windows XP con Service Pack 1</li> </ul>	<ul style="list-style-type: none"> <li>Nuovi aggiornamenti disponibili solo fino al mese di settembre 2006; aggiornamenti precedenti disponibili</li> </ul>
<ul style="list-style-type: none"> <li>Windows XP</li> </ul>	<ul style="list-style-type: none"> <li>Nuovi aggiornamenti disponibili solo fino al mese di settembre 2004; aggiornamenti precedenti disponibili</li> </ul>
<b>Windows 2000</b>	
<ul style="list-style-type: none"> <li>Windows 2000 con Service Pack 4</li> </ul>	<ul style="list-style-type: none"> <li>Attualmente supportato</li> </ul>
<ul style="list-style-type: none"> <li>Windows 2000 con Service Pack 3</li> </ul>	<ul style="list-style-type: none"> <li>Nuovi aggiornamenti disponibili solo fino al mese di giugno 2005; aggiornamenti precedenti disponibili</li> </ul>
<ul style="list-style-type: none"> <li>Windows 2000 con Service Pack 2</li> </ul>	<ul style="list-style-type: none"> <li>Nuovi aggiornamenti disponibili solo fino al mese di giugno 2004; aggiornamenti precedenti disponibili</li> </ul>
<ul style="list-style-type: none"> <li>Windows 2000 con Service Pack 1</li> </ul>	<ul style="list-style-type: none"> <li>Nuovi aggiornamenti disponibili solo fino al mese di agosto 2004; aggiornamenti precedenti disponibili</li> </ul>

<ul style="list-style-type: none"> <li>Windows 2000</li> </ul>	<ul style="list-style-type: none"> <li>Non più supportato</li> </ul>
<b>Sistemi operativi aggiuntivi</b>	
<ul style="list-style-type: none"> <li>Windows Millennium Edition</li> </ul>	<ul style="list-style-type: none"> <li>Aggiornamenti critici e della protezione successivi al mese di dicembre 2003; nuovi aggiornamenti disponibili solo fino al mese di giugno 2006</li> </ul>
<ul style="list-style-type: none"> <li>Windows 98</li> </ul>	<ul style="list-style-type: none"> <li>Aggiornamenti critici e della protezione successivi al mese di agosto 2002; nuovi aggiornamenti disponibili solo fino al mese di giugno 2006</li> </ul>
<ul style="list-style-type: none"> <li>Windows NT Server</li> </ul>	<ul style="list-style-type: none"> <li>Non più supportato dal mese di dicembre 2004</li> </ul>
<ul style="list-style-type: none"> <li>Windows NT Workstation</li> </ul>	<ul style="list-style-type: none"> <li>Non più supportato dal mese di giugno 2004</li> </ul>

Si può notare come nella tabella non venga citato Windows 95 per il quale non è più previsto alcun sviluppo e rilasciato alcun aggiornamento.

Con riferimento al **disciplinare tecnico** relativo alle **MISURE MINIME DI SICUREZZA**, il cui contenuto viene di seguito riportato in allegato, pare evidente come, alcune tipologie di Sistemi Operativi, **non risultino adeguati per rispettare tali misure MISURE MINIME DI SICUREZZA**.

Con riferimento alla regola **2-5-6-7** dell'allegato B) riferiti ai codici di autenticazione degli utenti, è noto che sui Sistemi Operativi quali Windows 95 e 98 pur se abilitata la password questa venga facilmente by-passata premendo semplicemente il tasto "**Esc**" (in fase di avvio del Sistema).

Tale superamento, oltre a non rispettare le indicazioni cogenti imposte dal Garante, non consentirà di accedere alle risorse di rete condivise (dischi di rete o sul server) ma permetterà il libero accesso al Desktop e alle risorse del Computer dell'utente.

Alla regola **17** si evidenzia la necessità di aggiornamenti periodici da adottare sui programmi e Sistemi Operativi volti a prevenire la vulnerabilità degli strumenti elettronici correggendone i difetti; in tale ottica è evidente come ne Windows 95, 98 ne Windows NT possono rispettare la regola **17** poichè Microsoft non rilascia/sviuppa aggiornamenti per tali Sistemi Operativi.

## Supporto Tecnico

**IPSlab srl** Contrà Porti, 16  
36100 VICENZA  
<http://www.ipslab.it> e-mail.: [supporto@ipslab.it](mailto:supporto@ipslab.it)  
Tel.: 333.800.8008 Fax.: 0444.809852

Autore: D.S.	Data di emissione: 17/12/04	Riclassificazione: 15/10/05
Proprietario: IPSlab srl	- PUBBLICO -	
Cod. doc. : SO_Superati	Tutti i diritti riservati	
		<b>2 di 7</b>

ALLEGATO B  
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

Autore: D.S.	Data di emissione: 17/12/04	Riclassificazione: 15/10/05
Proprietario: IPSlab srl	- PUBBLICO -	3 di 7
Cod. doc. : SO_Superati	<i>Tutti i diritti riservati</i>	

## **ALLEGATO B**

### **DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice)**

#### **Trattamenti con strumenti elettronici**

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

#### **Sistema di autenticazione informatica**

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
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.
5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
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.

Autore: D.S.	Data di emissione: 17/12/04	Riclassificazione: 15/10/05
Proprietario: IPSlab srl	- PUBBLICO -	4 di 7
Cod. doc. : SO_Superati	Tutti i diritti riservati	

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

### **Sistema di autorizzazione**

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

### **Altre misure di sicurezza**

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

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, 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**.

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

### **Documento programmatico sulla sicurezza**

19. **Entro il 31 marzo di ogni anno**, 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:**

19.1. **l'elenco dei trattamenti di dati personali;**

19.2. **la distribuzione dei compiti e delle responsabilità** nell'ambito delle strutture preposte al trattamento dei dati;

19.3. **l'analisi dei rischi che incombono sui dati;**

19.4. **le misure da adottare per garantire l'integrità** e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di **interventi formativi degli incaricati del trattamento**, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati

personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti

di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

### **Ulteriori misure in caso di trattamento di dati sensibili o giudiziari**

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615- *ter* del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

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.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

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 superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

### **Misure di tutela e garanzia**

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella **relazione accompagnatoria del bilancio d'esercizio**, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

### **Trattamenti senza l'ausilio di strumenti elettronici**

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

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

Autore: D.S.	Data di emissione: 17/12/04	Riclassificazione: 15/10/05
Proprietario: IPSlab srl	- PUBBLICO -	6 di 7
Cod. doc. : SO_Superati	Tutti i diritti riservati	

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.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Autore: D.S.	Data di emissione: 17/12/04	Riclassificazione: 15/10/05
Proprietario: IPSlab srl	- PUBBLICO -	7 di 7
Cod. doc. : SO_Superati	Tutti i diritti riservati	