CHECK LIST PER LE VERIFICHE SULL'OPERATO DEGLI AMMINISTRATORI DI SISTEMA

Una proposta per rispondere alla misura 4.4 (o "e") del Provvedimento del Garante del 28 novembre 2008.

E' possibile dare il proprio contributo e diffonderla a chiunque secondo la licenza
http://creativecommons.org/licenses/by-nc/2.5/it/

Introduzione

Ogni misura è preceduta da una sigla ed un numero, secondo i criteri che seguono:

- B.n: misura presente nell'Allegato B del Dlgs 196/2003
- AdS.n: misura presente nel Provvedimento del Garante del 28 novembre 2008 (Amministratori di Sistema)
- G.n: misura presente in altri provvedimenti o linee guida del Garante, tra cui:
  - Delibera numero 13 del 1 marzo 2007 (Linee guida per posta elettronica e Internet)
  - Provvedimento del 8 aprile 2010 (Videosorveglianza)

Attività preliminare

Attività preliminare è il censimento di:

- Sistemi Operativi (inclusi quelli virtuali)
- Applicazioni (sia di tipo "business" come i gestionali, sia di tipo "supporto" come le email)
- Apparati e sistemi di rete (es. firewall, proxy, eccetera)

Check list

MISURE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI

MISURA	NOTE	C/NC
B.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	Verificare con gli AdS come è impostato tale controllo su tutte le tipologie di sistemi (Win, *x, mainframe, eccetera). Verificare che analoghe procedure sono attuate anche per gli AdS.	
B.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.	Vedere B.1. Particolarmente importante per gli accessi dei power-users.	
B.3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.	Vedere B.1	
B.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.	Verificare la presenza delle istruzioni, che siano conosciute anche dagli AdS.	
B.5 (a). 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.	Verificare la configurazione dei sistemi che abbiamo opportunamente impostate le policy di sicurezza delle password.	
B.5 (b). La parola chiave è modificata dall'incaricato al primo utilizzo.	Verificare la configurazione dei sistemi che abbiamo opportunamente impostate le policy di sicurezza delle password. Chiedere agli AdS le modalità di inserimento dei nuovi utenti e di reset delle password quando dimenticate.	

MISURA	NOTE	C/NC
B.5 (c). La parola chiave è modificata dall'incaricato almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.	Verificare la configurazione dei sistemi che abbiamo opportunamente impostate le policy di sicurezza delle password.	
B.6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.	Verificare la configurazione dei sistemi. Particolarmente rilevante è comprendere come sono utilizzate le utenze di amministrazione (Admin, root, eccetera) per ogni tipologia di sistema (apparati di rete inclusi). Verificare i log di accesso se presentano numerosi accessi da parte dell'utenza generica di amministrazione. Si considerino le necessarie eccezioni dovute ad esigenza puramente tecniche. Verificare se è strutturato (con procedura e conseguenti registrazioni) un processo di assegnazione e revoca delle utenze in modo da analizzare eventuali scostamenti da quanto prescritto	
B.7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.	Verificare la configurazione dei sistemi.	
B.9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.	Verificare che gli AdS dispongano di tali istruzioni.	
B.12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.	Verificare la configurazione dei sistemi. Normalmente gli AdS possono avere pieno accesso a tutti i dati, ma vanno comunque controllate le corrette impostazioni dei sistemi e delle applicazioni.	
B.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.	Verificare che gli AdS abbiano tutte le informazioni necessarie per configurare opportunamente i sistemi: ticket, email, manuali a seconda delle procedure aziendali. Esempio di modalità di verifica: individuare un utente (incaricato) e verificare se gli sono assegnati i soli privilegi previsti.	
B.14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.	Verificare le modalità con cui tale requisito è affrontato.	
B.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.	Verificare che gli AdS abbiano tutte le informazioni necessarie per configurare opportunamente i sistemi.	
AdS.2. La designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.	Verificare l'elenco degli AdS e la corrispondenza con le utenze di power user (root, admin, etc) sui vari sistemi. Verificare che sui diversi server o apparati siano presenti i soli power user previsti.	
AdS.3 (a). Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile.	Verificare l'elenco degli AdS e la corrispondenza con le utenze di power user sui vari sistemi.	
AdS.3 (b). Qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, i titolari sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni.	Verificare che sia presente e opportunamente pubblicato l'elenco degli AdS con accesso ai dati dei lavoratori. Verificare la corrispondenza di questo elenco con le utenze di power user sui vari sistemi.	
AdS.6 (a). Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.	Verificare la configurazione dei sistemi. Analizzare chi e come può accedere ai log, con quali permessi e se può modificarli.	
AdS.6 (b). Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste.	Verificare la configurazione dei sistemi. Analizzare chi e come può accedere ai log, con quali permessi e se può modificarli.	

MISURA	NOTE	C/NC
AdS.6 (c). Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi	Verificare la configurazione dei sistemi. Analizzare chi e come può accedere ai log, con quali permessi e se può modificarli.	
AdS.5. L'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento o dei responsabili, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.	Questa check-list è la risposta a questo requisito	
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), mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.	Verificare la configurazione dei sistemi, inclusi i pc degli AdS.	
B.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.	Verificare la configurazione dei sistemi, inclusi i pc degli AdS.	
B.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.	Verificare la configurazione dei sistemi (in particolare la presenza di firewall quando connessi alla rete). Di particolare rilievo i pc degli utenti e degli AdS.	
B.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	Verificare la disponibilità di tali istruzioni agli AdS.	
B.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	Verificare che gli AdS abbiano strumenti idonei alla cancellazione sicura dei supporti (allineati con le istruzioni di cui sopra).	
B.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	N/A per gli AdS.	
B.26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza	N/A per gli AdS.	

MISURE PER GARANTIRE LA PROTEZIONE DELLE AREE E DEI LOCALI

MISURA	NOTE	C/NC
B.27 (b). 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.	Questa misura riguarda gli archivi non elettronici. Non applicabile per gli AdS.	
B.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.	N/A per gli AdS. E' comunque possibile verificarne l'applicazione nei locali di loro pertinenza.	
B.29 (a). 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.	N/A per gli AdS. E' comunque possibile verificarne l'applicazione nei locali di loro pertinenza.	
B.29 (b). 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.	Verificare come sono gestiti gli strumenti elettronici per il controllo degli accessi: anche loro avranno degli AdS. E' inoltre possibile verificarne l'applicazione nei locali di pertinenza degli AdS.	
B.19.4. Garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità	N/A per gli AdS. E' comunque possibile verificarne l'applicazione nei locali di loro pertinenza.	

CRITERI E MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

MISURA	NOTE	FAM.
B.10 (a). 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.	Verificare la disponibilità di tali istruzioni. Verificare la loro applicazione. Verificare se il caso si è presentato e chiedere come si sono svolte le operazioni.	
B.10 (b) 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.	Verificare la disponibilità di tali istruzioni. Verificare la loro applicazione.	
B.18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.	Verificare la disponibilità di tali istruzioni. Verificare la loro applicazione.	
B.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.	Verificare la disponibilità di tali istruzioni. Verificare la loro applicazione. Chiedere se sono stati effettuati dei test di ripristino.	

CRITERI IN CASO DI TRATTAMENTI AFFIDATI ALL'ESTERNO DELLA STRUTTURA

MISURA	NOTE	C/NC
B.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 dell'Allegato B del Dlgs 196/2003.	Verificare le modalità di coinvolgimento degli AdS in merito. Verificare se gli AdS sono a loro volta dei soggetti esterni e, quindi, come viene regolato il rapporto e se (in quanto installatori) mantengono le descrizioni scritte richieste.	
B.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;	N/A per gli AdS	
AdS.4. Nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare o il responsabile esterno devono conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.	Verificare la presenza di tali liste e il loro stato di aggiornamento.	

INTERVENTI FORMATIVI E ORGANIZZATIVI

MISURA	NOTE	C/NC
B.19.6(b). Tutto il personale deve essere formato 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.	Verificare se gli AdS sono stati opportunamente formati.	
B.19.6(b). 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;	N/A per gli AdS.	
AdS.1. L'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.	Due elementi: 1. Verificare le registrazioni sulle esperienze e capacità (esempio CV). 2. Verificare come sono state condotte le valutazioni da parte del Responsabile o Titolare (es. valutazione periodica del personale o anche un "visto" nell'elenco degli AdS.	
G.1. E' distribuito a tutto il personale un disciplinare interno sull'uso dell'e-mail e di Internet da parte dei lavoratori	Verificare la presenza di tale disciplinare anche agli AdS.	

VIDEOSORVEGLIANZA

MISURA	NOTE	C/NC
G.V1 Gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata utilizzando il modello semplificato (cartello "Area Videosorvegliata".	N/A per AdS	
G.V2 In presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini. Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i predetti soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;	Verificare se e come sono trattati i sistemi di videosorveglianza. Nel caso siano basati su supporti informatici, le norme per gli AdS sono applicabili. Verificare la configurazione dei sistemi.	
G.V3 Laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione	Verificare la configurazione dei sistemi. Verificare se si sono verificati dei casi e come sono stati gestiti.	
G.V4 Per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto	Verificare la configurazione dei sistemi.	
G.V5 Nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle predette operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini	Verificare la configurazione dei sistemi. Verificare se si sono verificati dei casi e come sono stati gestiti.	
G.V6 Qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del codice penale	Verificare la configurazione dei sistemi. (antivirus)	
G.V7 La trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless	Verificare la configurazione dei sistemi.	

MISURA	NOTE	C/NC
G.V8 Gli impianti e le apparecchiature, dai quali può derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti	N/A per gli AdS.	
G.V9 Nel caso in cui trovi applicazione la disciplina del Codice, il trattamento di dati può essere lecitamente effettuato da privati ed enti pubblici economici solamente se vi sia il consenso preventivo dell'interessato, oppure se ricorra uno dei presupposti di liceità previsti in alternativa al consenso	N/A per gli AdS.	

Introduzione

Al documento ha collaborato Vito Losacco.