ALLEGATO LL (art. 474, c. 7)([1])

DISCIPLINARE TECNICO PER AMMINISTRATORI DI SISTEMA

Premessa

Il presente disciplinare tecnico descrive le basilari regole tecniche ed organizzative che gli amministratori di sistema devono applicare per garantire la sicurezza dei dati e delle informazioni trattate con l'utilizzo di strumentazioni informatiche nella Regione.

Tenendo conto di quanto esplicitato nel Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 (Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema) pubblicato sulla G.U. n. 300 del 24.12.2008, e successive modificazioni, la definizione di "amministratori di sistema", ai fini dell'applicazione del presente disciplinare, è la seguente:

"sono le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (quali ad es. gli amministratori di dominio e di server), nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi."

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni), nelle loro consuete attività sono, in molti casi, concretamente «responsabili» di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti «in chiaro» le informazioni medesime.

Pertanto, considerata la delicatezza di tali peculiari mansioni e i rischi ad esse associati, la designazione di un amministratore di sistema non può prescindere da alcune considerazioni e accorgimenti:

a) valutazione delle caratteristiche soggettive: 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;

b) designazioni individuali: 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;

c) elenco degli amministratori di sistema: 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 in caso di accertamenti anche da parte del Garante. Qualora l'attività

[1] Allegato inserito dall'art. 6, comma 1, del r.r.2 novembre 2020, n.27, pubblicato sul BUR Lazio 3 novembre 2020, n.132

degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori, la Regione rende nota o conoscibile l'identità degli amministratori di sistema con comunicazione effettuata nell'ambito del portale di comunicazione interna Intranet;

d) servizi in outsourcing: nel caso di servizi di amministrazione di sistema affidati in outsourcing la Regione conserva, presso la direzione competente in materia di Sistemi Informativi, ognuno per la parte di propria competenza, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;

e) verifica delle attività: l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del titolare del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti;

f) registrazione degli accessi: 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. 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.

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.

Ai fini del presente disciplinare, si intende per sistema informativo il complesso dei dati, delle applicazioni, delle risorse tecnologiche, delle risorse umane, delle regole organizzative e delle procedure deputate all'acquisizione, memorizzazione, consultazione, elaborazione, conservazione, cancellazione, trasmissione e diffusione delle informazioni. Esempi di sistemi informativi sono server (file, database, web, mail, ecc.), applicazioni, apparati di rete (router, switch, ecc.), strumenti di sicurezza (firewall, IPS, ecc.).

Applicabilità

Le regole illustrate nel disciplinare tecnico si applicano a tutti i dipendenti appartenenti all'organico della Regione e a tutti coloro che a vario titolo svolgono attività, compiti, mansioni come amministratori di sistema.

Principi generali

È compito di ogni amministratore di sistema comprendere le minacce di sicurezza incombenti sui propri sistemi e adottare le contromisure di sicurezza necessarie ad assicurare confidenzialità, integrità e disponibilità dei dati e delle informazioni.

A titolo esemplificativo tali minacce possono essere:

- *minacce incombenti sui dati* (furto di dati, incluse credenziali di accesso a basi dati; distruzione anche accidentale di dati; modifica di dati, anche intenzionale, per introdurre informazioni false e fuorvianti);
- *minacce incombenti sulle applicazioni e sui sistemi operativi* (attacchi di vario tipo quali virus, spamming, SQL injection, Denial of Service; accessi non autorizzati, anche non intenzionali);

- *minacce incombenti sull'infrastruttura* (furto di apparecchiature; danneggiamento/distruzione di apparecchiature sia intenzionale che accidentale; smarrimento di apparecchiature o credenziali; reazione inadeguata ad incidenti/disastri).

Sicurezza fisica

L'accesso fisico ai locali della Regione è regolato dall'apposito disciplinare tecnico regionale in materia.

La scelta dei locali in cui installare, conservare o utilizzare sistemi informatici deve essere fatta tenendo in considerazione i potenziali rischi di sicurezza sui dati causati tanto da eventi accidentali quanto da dolo. In funzione dell'analisi dei rischi devono essere valutate e adottate idonee misure di protezione, quali sistemi di antintrusione, sistemi antincendio, sistemi di rilevazione fumi, sistemi antiallagamento.

La scelta delle misure di sicurezza dei locali deve, in ogni caso, tenere conto dei vincoli imposti dalla normativa in materia di tutela della salute e di sicurezza dei lavoratori.

La protezione dei server e degli apparati di rete considerati critici per il funzionamento e la disponibilità dei sistemi informativi deve prevedere sistemi di protezione elettrica quali stabilizzatori di corrente ed apparecchiature UPS e sistemi di condizionamento dell'aria nei locali per garantire il mantenimento di una costante ed adeguata temperatura di esercizio.

La scelta dei locali per gli armadi deve essere fatta individuando ambienti idonei, possibilmente dedicati e ad accesso limitato (solo agli amministratori di sistema e ad un eventuale custode incaricato). Gli armadi medesimi devono essere chiusi a chiave e le relative chiavi devono essere in possesso dei soli amministratori di sistema (e di un eventuale custode specificatamente incaricato). Le chiavi di accesso a locali o armadi possono essere conservate presso le portinerie della Regione.

Controllo dell'accesso ai dati

L'accesso ai dati ed alle strumentazioni informatiche utilizzate per trattarli deve essere concesso al solo personale espressamente autorizzato (nel caso di dati personali i cosiddetti incaricati del trattamento). L'elenco del personale incaricato deve essere aggiornato almeno a cadenza annuale.

In nessun modo devono essere concessi permessi di accesso ai sistemi senza preventiva autorizzazione formale del responsabile funzionale o del referente regionale di progetto. Le modalità con cui viene formulata tale autorizzazione possono variare a seconda del tipo di trattamento.

Autenticazione

L'accesso ai dati trattati con strumentazioni informatiche deve essere concesso esclusivamente previa opportuna autenticazione.

Gli strumenti di autenticazione devono essere progettati in funzione del valore dei dati trattati. Deve essere prevista l'ipotesi di utilizzo di sistemi di autenticazione forte ove necessario (smart card, token hardware, dispositivi one-time password, sistemi biometrici).

Devono essere previsti meccanismi di separazione dei privilegi, sia a livello di sistema operativo che a livello applicativo, per consentire l'accesso ai dati e le operazioni effettuate sugli stessi, in misura corrispondente ai diversi profili degli utenti.

Autorizzazione
È necessario introdurre dei criteri generali di definizione dei ruoli amministrativi e di gestione delle autorizzazioni, pur nel pieno rispetto dei principi di delega e di autonomia dei referenti di applicazioni e sistemi che gestiscono porzioni del sistema informativo.

Il principio generale a cui attenersi è che i ruoli amministrativi critici non si devono sovrapporre. Ad esempio, gli sviluppatori non devono essere anche sistemisti, gli amministratori della sicurezza non devono essere sistemisti o sviluppatori e così via. Qualora non fosse possibile dal punto di vista organizzativo mantenere o adottare questa separazione di ruoli, devono essere introdotti controlli compensativi che permettano di tracciare puntualmente le operazioni eseguite (ad esempio tramite l'utilizzo di strumenti evoluti di monitoraggio, audit puntuali, notifiche via e-mail).

Gestione delle credenziali
Le credenziali consentono all'utente di accedere ai dati e pertanto è necessario che la loro assegnazione segua procedure codificate e condivise. Tali procedure possono essere diverse in funzione sia del valore dei dati da trattare che dei sistemi coinvolti.

In generale, le richieste delle credenziali di autenticazione devono essere fatte dai responsabili funzionali o referenti regionali di progetto. In ogni caso, deve essere tenuta traccia della richiesta che ha generato la creazione di una credenziale di autenticazione sul sistema. Le modalità con cui sono formulate le richieste variano in funzione della criticità dei dati o dei sistemi (per esempio e-mail, lettera protocollata, determinazione).

Ogni credenziale di autenticazione deve riferirsi ad un singolo utente. Non è consentito l'utilizzo di credenziali condivise. Fanno eccezione a questa regola le credenziali amministrative di accesso ai sistemi (es. root, administrator), che devono comunque essere assegnate ad un numero limitato di incaricati e devono essere utilizzate solo nel caso di interventi particolari sui sistemi. Ove possibile, bisogna privilegiare sempre l'utilizzo di credenziali nominative anche nel caso di operazione di amministrazione dei sistemi.

La gestione delle credenziali deve seguire le procedure documentate per i vari sistemi di autenticazione. La policy di scadenza delle credenziali non utilizzate è normalmente di 180 giorni. Fa eccezione a questa regola il dominio applicativo esterno per la peculiarità di alcune applicazioni che sono utilizzate dagli utenti con periodicità annuale: in questo caso le credenziali non utilizzate sono disabilitate dopo un anno. Le policy di gestione delle password devono essere allineate sui diversi sistemi e comunque conformi ai dettami delle norme in materia di protezione dei dati personali.

Le credenziali amministrative non nominative di gestione dei sistemi non sono vincolate alle stesse regole delle credenziali nominative, non scadono dopo un periodo di inutilizzo, non vengono bloccate dopo un certo numero di tentativi errati, non hanno la password che scade e non ne viene richiesta la modifica al primo accesso. Perciò gli amministratori dei sistemi sono tenuti ad adottare politiche manuali di modifica delle password dei loro sistemi e a monitorare gli eventuali tentativi di accesso non autorizzato. Le credenziali amministrative non nominative create al solo scopo di avviare servizi sui server non devono poter effettuare l'accesso interattivo sui sistemi stessi o, ove ciò non fosse tecnologicamente possibile, deve essere comunque monitorato il loro utilizzo per scopi diversi rispetto all'ambito per cui sono state create.

Le credenziali di autenticazione con privilegi amministrativi non devono essere inviate via e-mail: in tali casi, è necessario convocare l'utente e fornirgli le credenziali verbalmente, oppure mediante un sistema di scambio informazioni sicuro.

Gli amministratori dei sistemi sono tenuti a rispettare le procedure adottate e a non creare particolarità o eccezioni nella gestione delle credenziali utente.

La gestione delle credenziali amministrative deve seguire regole molto rigide e stringenti: devono essere identificate le persone autorizzate a richiedere l'aggiunta o la modifica di amministratori dei sistemi o delle applicazioni e deve essere previsto un sistema di notifica che avvisi gli altri amministratori del cambiamento.

In generale una procedura di gestione delle credenziali deve prevedere:

a)l'identificazione di chi può chiedere la creazione, la modifica, la disabilitazione, la cancellazione di un'utenza, le operazioni di sblocco dell'utente o il reset della password; tale identificazione, qualora avvenga tramite telefono, deve essere fatta chiedendo alcuni dati personali al richiedente;

b)la modalità di inoltro della richiesta: alcune operazioni quali la creazione o la modifica dovranno essere fatte via e-mail o fax, altre quali il reset della password potranno anche essere fatte verbalmente dall'utente interessato tramite telefono, previa la verifica da parte degli amministratori dell'identità dell'interessato (es. tramite richiesta di alcuni dati personali);

c)l'elenco dei destinatari della richiesta: ad esempio i referenti dell'applicazione, gli amministratori dei sistemi, il servizio di help desk;

d)la tempistica di evasione della richiesta;

e)l'archiviazione e il backup delle richieste pervenute via e-mail e delle risposte relative all'attività svolta. Se la richiesta è in formato cartaceo deve essere acquisita agli atti;

f)la modalità di risposta al richiedente per comunicare l'avvenuta attivazione dell'utenza, il nome utente e la password (a tale proposito valutare se sia opportuno crittografarla, ovvero comunicarla verbalmente all'utente, ove possibile).

Le procedure di gestione delle credenziali debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Gestione delle password
La lunghezza minima consentita per le password deve essere impostata ad almeno otto caratteri. Ove la tecnologia non lo consenta, la lunghezza delle password deve essere impostata al massimo consentito dal sistema.

La durata della password dovrebbe essere impostata in base al grado di criticità di sistemi e basi dati. Inoltre, una eventuale password di "single sign on" è opportuno abbia una durata inferiore a quella delle password che sostituisce.

Per contrastare attacchi alle password di tipo "brute-force" i sistemi informatici devono prevedere opportuni meccanismi per la disabilitazione di un account dopo un intervallo finito di tentativi di accesso non riusciti. Devono comunque essere previsti meccanismi di difesa da attacchi di tipo *denial of service* causati dal blocco volontario di account legittimi. Un esempio di tali meccanismi di difesa è di consentire per un account un limite massimo di cinque tentativi di accesso non riusciti, prevedendo il blocco dell'account per un periodo di trenta minuti nel caso in cui tale limite venga superato.

Ove tecnologicamente possibile, deve essere data agli utenti la possibilità di modificare la propria password senza l'intervento degli amministratori.

Devono essere previsti meccanismi di implementazione dei sistemi tali da garantire all'utente la modifica della propria password al primo accesso al sistema.

Le password non devono essere conservate in chiaro, né trasmesse su canali non cifrati. Per la loro conservazione devono essere utilizzati adeguati meccanismi di cifratura anche in funzione del valore dei dati, per esempio, hash calcolati con funzioni irreversibili per la conservazione su disco; analogamente per la loro trasmissione devono essere utilizzati protocolli di comunicazione cifrati come SSL.

In caso di trattamento di dati sensibili (articolo 9 del RGPD) e/o giudiziari (articolo 10 del RGPD) o comunque di rilevanza strategica, devono essere previsti sistemi di controllo delle password per consentire il solo utilizzo di password "resistenti" ad attacchi "brute-force". Per esempio, password formate con valori alfanumerici maiuscoli e minuscoli, simboli e caratteri speciali.

Al momento dell'installazione, su tutti i sistemi, devono essere modificate le password di default utilizzate dal produttore/installatore.

Protezione dei dati

Backup

Per garantire la disponibilità dei dati devono essere previste idonee procedure di backup in funzione del valore dei dati trattati. Tali procedure devono essere formalizzate per iscritto e tenute aggiornate con cadenza almeno annuale.

Con cadenza periodica (perlomeno annuale) devono essere effettuati controlli a campione (su un campione opportunamente numeroso: es. una copia per ogni mese) sulle copie di backup per verificarne la disponibilità e l'integrità.

A fronte di cambiamenti intervenuti nel sistema di backup o nei sistemi che devono essere archiviati devono essere fatti dei test di backup e restore per verificare la consistenza dei dati salvati.

Tutti i test vanno documentati in un "diario" che riporti la data del test, il sistema coinvolto, la persona che ha eseguito il test e l'esito delle operazioni effettuate.

Le copie di backup devono essere conservate in locali fisicamente separati da quelli dei sistemi origine dei dati, per garantire la disponibilità delle copie in caso di eventi accidentali quali incendi o disastri naturali. Le copie dei backup devono essere riposte, possibilmente, in casseforti le cui chiavi sono conservate da personale identificato. L'elenco del personale autorizzato deve essere regolarmente mantenuto aggiornato.

Gli amministratori devono censire e tenere aggiornate le informazioni sul backup dei sistemi da loro gestiti. In particolare, devono richiedere alla struttura competente l'attivazione del backup per i nuovi sistemi e applicazioni e devono segnalare esigenze particolari di backup che esulino dalle politiche in essere di backup centralizzato.

Gli amministratori del sistema di backup devono monitorare l'esito deitask eseguiti e, qualora rilevassero problemi, darne pronta segnalazione agli amministratori dei sistemi coinvolti.

Il sistema di backup, sia per quanto riguarda il software di base che il software applicativo, deve essere mantenuto aggiornato, in particolare relativamente alle patch/hot-fixes di sicurezza. Qualora venissero rilasciate patch/hot-fixes di sicurezza per la parte client, gli aggiornamenti sui singoli sistemi devono essere pianificati in accordo con gli amministratori degli stessi.

Le politiche di backup debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Procedure di dismissione dei sistemi: protezione dei dati
Ogni qualvolta si dismette un dispositivo elettronico o informatico che contiene dati personali, è necessario adottare idonei accorgimenti e misure, anche attraverso soggetti terzi, tecnicamente qualificati, che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

Chi procede al riutilizzo di dispositivi elettronici o informatici è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo ove possibile, l'autorizzazione a cancellarli o a renderli non intellegibili.

Il processo di rimozione dei dati dai dischi dei computer è denominato *disk sanitizing*, *cleaning*, *purging*, o *wiping*. Il metodo scelto per "disinfettare" un disco dipende dalla criticità dei dati in esso contenuti.

Cancellare un file comporta in effetti la sola rimozione del puntatore al file. Esistono strumenti software in grado di recuperare file cancellati e quindi i dati in essi contenuti. Pertanto, per garantire la cancellazione sicura delle informazioni le tecniche possibili sono:

- Sovrascrittura: il numero di ripetizioni del procedimento considerato sufficiente a raggiungere una ragionevole sicurezza (da rapportarsi alla delicatezza delle informazioni di cui si vuole impedire l'indebita acquisizione) varia e incide proporzionalmente sui tempi delle procedure;
- Formattazione "a basso livello" (LLF) dei dispositivi di tipo hard disk, laddove possibile, attenendosi alle istruzioni fornite dal produttore e tenendo conto delle possibili conseguenze tecniche su di esso, fino alla possibile sua successiva inutilizzabilità;
- Smagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici, in grado di garantire la cancellazione rapida delle informazioni anche su dispositivi non più funzionanti sui quali potrebbero non essere applicabili le procedure di cancellazione software;
- Distruzione fisica dei dispositivi.

La sovrascrittura è in genere sufficiente a garantire che i dati prima presenti non siano più recuperabili e dunque leggibili.

Smagnetizzare o distruggere fisicamente il disco garantisce l'inutilizzabilità futura del disco medesimo e dunque previene qualsiasi tentativo di recupero dei dati.

Le procedure utilizzate in caso di reimpiego o di smaltimento dei dispositivi e degli strumenti informatici debbono essere documentate, mantenute aggiornatee messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Protezione delle applicazioni

Design, sviluppo, deployment e gestione

Le applicazioni devono essere sviluppate dispiegate e gestite secondo i principi di privacy by design e privacy by default, secondo quanto definito da specifico disciplinare.

Protezione dei sistemi

È compito di ogni amministratore mantenere un elenco aggiornato e completo delle risorse gestite. L'elenco, nel caso di server, deve contenere almeno:

- i riferimenti fisici e logici del server (nome e indirizzo di rete), la sua ubicazione e i riferimenti relativi al backup;
- le versioni dell'hardware e del sistema operativo;
- le funzioni e applicazioni principali oppure il ruolo all'interno dell'infrastruttura regionale.

Precedentemente alla progettazione, implementazione, installazione o gestione di un sistema, deve essere effettuata un'analisi dei rischi per determinare le misure di sicurezza da adottare.

Tutti gli interventi tecnici che coinvolgono la creazione, modifica o eliminazione di uno dei meccanismi di sicurezza indicati nel disciplinare tecnico, devono essere opportunamente documentati ed autorizzati da parte del proprio referente funzionale.

Server

Gli amministratori dei sistemi server devono tener conto delle seguenti policy generali e devono documentare qualsiasi eccezione a queste regole.

Policy generale

1. Hardware, sistemi operativi, servizi ed applicazioni installati devono essere approvati dalla direzione competente in materia di Sistemi Informativi.

2. Tutte le patch/hotfixes di sicurezza rilasciate dai fornitori devono essere installate nel minor tempo possibile valutando a priori, in base al rischio, la verifica in ambiente di pre-produzione. Sono ammesse eccezioni basate su specifiche esigenze di servizio della Regione, adeguatamente giustificate, documentate e riportate dagli amministratori alla direzione competente in materia di Sistemi Informativi. I servizi non necessari devono essere rimossi/disabilitati, compatibilmente con le dipendenze del sistema in oggetto. È compito degli amministratori mantenersi costantemente aggiornati sulle patches/hotfixes da installare.

3. Servizi non sicuri devono essere sostituiti da equivalenti oggetti sicuri, ove ciò sia possibile. Peresempio servizi con traffico in chiaro (telnet) devono essere sostituiti da servizi con traffico cifrato (SSH).

4. Relazioni di fiducia tra sistemi possono essere configurate solo per specifiche esigenze di servizio. Devono essere documentate dagli amministratori ed approvate dalla direzione competente in materia di Sistemi Informativi.

5. Qualsiasi attività di amministrazione remota deve essere effettuata utilizzando canali sicuri (es. connessioni di rete con crittografia, che utilizzino SSH o IPSEC). Qualora non sia disponibile una modalità di accesso remoto sicuro, dovrebbero essere utilizzate "one-time" password per tutti i livelli di accesso.

6. I server di produzione devono essere fisicamente localizzati in un ambiente ad accesso controllato, con un impianto di condizionamento adeguato alle esigenze, ovvero in grado

di mantenere la temperatura e l'umidità entro i limiti che consentono la normale operatività dei server.

7. È vietata l'installazione di hardware e software non autorizzato. Tutte le attività di modifica di hardware o software devono essere preventivamente autorizzate, preferibilmente mediante definizione e schedulazione delle attività di aggiornamento (upgrade sistema operativo, modifica hardware, ecc.).

8. Tutti i server di produzione devono essere collegati ad un sistema di UPS (UninterruptiblePowerSupplies) più Gruppo Elettrogeno oppure solo UPS che consenta una disconnessione (shutdown) automatica dei server prima dell'esaurimento delle batterie.

Le modalità operative di installazione, configurazione ed aggiornamento, debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Apparati di rete
Gli amministratori di rete, nell'attività di configurazione e gestione degli apparati di rete di produzione, devono basarsi sulle seguenti regole generali e documentare le eventuali deroghe o eccezioni.

Policy generale

1. Tutti i router dovrebbero usare un protocollo di accounting per autenticare gli utenti. L'accesso con account locali è consentito solo in situazioni d'emergenza ovvero quando non fosse disponibile il sistema centralizzato di autenticazione.

2. La password di enable deve essere configurata utilizzando il meccanismo di "enable secret" che ne permette la cifratura sicura.

3. Disabilitare le seguenti funzioni (alcuni termini inglesi non sono stati tradotti perché così sono conosciuti in ambito tecnico):

- IP directed broadcast;
- pacchetti in ingresso con indirizzi non validi come da RFC1918;
- TCP small services;
- UDP small services;
- tutti i sourcerouting;
- tutti i servizi web;
- Protocollo CDP o similari.

4. Usare la community SNMP adottata dalla Regione e comunque diversa da *public* o *private*, oppure limitare l'accesso agli apparati impostando opportuni filtri.

5. Le regole di accesso devono essere aggiunte o modificate aderendo alle necessità della Regione.

6. I router devono avere un banner di login che notifichi a chi accede che l'apparato è proprietà della Regione e che l'accesso è consentito al solo personale autorizzato.

7. Gli apparati di rete devono essere inclusi nel sistema di gestione dei sistemi di produzione adottato dalla Regione e quindi censiti riportando i riferimenti dei responsabili tecnici.

8. Deve essere utilizzato il protocollo SSH per gestire i router.

Le modalità operative di installazione, configurazione ed aggiornamento, come pure gli schemi della rete debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Postazioni di lavoro
Gli amministratori dei client devono tener conto delle policy generali di cui all'articolo 474 bis, comma 1, lettera e), del presente regolamento, relative alle postazioni di lavoro e devono documentare qualsiasi eccezione a queste regole.
Policy generale

1. Il software utilizzato sulle postazioni di lavoro deve essere associato ad una licenza, in accordo con le specifiche del fornitore/produttore;

2. Le postazioni di lavoro assegnate al personale dell'Ente devono essere utilizzate solo per gli scopi designati;

3.E'vietato installare hardware e software addizionale senza autorizzazione della direzione competente in materia di Sistemi Informativi ed è vietato alterare o cancellare software o modificare configurazioni su una postazione di lavoro della Regione senza autorizzazione da parte della medesima direzione.

4. Le modalità operative di installazione, configurazione ed aggiornamento, debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Dispositivi portatili
I dispositivi portatili seguono le stesse policy indicate per le postazioni di lavoro con un'attenzione maggiore alla protezione dei dati personali e alla tutela rispetto ai possibili tentativi di furto.

In caso di furto o smarrimento di un dispositivo portatile, l'amministratore di tali dispositivi deve agire tempestivamente, anche su segnalazione verbale del possessore, previa verifica dell'identità dello stesso tramite, ad esempio, la richiesta di alcuni dati identificativi personali (es. matricola, codice fiscale, ecc.).

Policy generale

Impostare la password di accesso al BIOS su tutti i dispositivi. Disabilitare, inoltre, da BIOS il boot da supporto rimovibile. Se il firmware consente di proteggere con password l'hard disk, e se lo si ritiene necessario per casi particolari e documentati, si abiliti anche questa funzionalità. La medesima password per BIOS e hard disk deve essere utilizzata su tutti i dispositivi, per accelerare gli interventi tecnici approvati.

I dispostivi portatili non devono essere lasciati in ufficio ma devono essere portati via al termine dell'orario di lavoro.

Le modalità operative di installazione, configurazione ed aggiornamento debbono essere documentate, mantenute aggiornate e messe a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.

Gestione dei log

È compito di ogni amministratore monitorare costantemente i sistemi gestiti per prevenire e limitare gli effetti di eventuali incidenti di sicurezza. Il metodo principale per effettuare il monitoraggio è costituito dalla raccolta ed analisi dei file di log.

La definizione ed il rilevamento degli eventi di sistema deve essere effettuata in funzione del valore dei dati ed in modo tale da consentire la verifica dell'efficacia e dell'efficienza delle procedure di sicurezza. Ove possibile devono comunque essere rilevati:

- autenticazione (login e logout, riusciti e non);
- accesso ai dati classificati sensibili dal punto di vista della sicurezza (lettura e scrittura);
- modifica di funzioni amministrative (es. la disabilitazione delle funzioni di logging,la gestione dei permessi, ecc.);
- connessioni di rete (in ingresso ed in uscita).

Ove possibile ogni voce di log deve contenere:

- data/ora dell'evento;
- luogo dell'evento (macchina, indirizzo IP, ecc.);
- identità dell'utente;
- identificativo del processo che ha generato l'evento;
- connessioni di rete (in ingresso ed in uscita) relative all'evento;
- descrizione dell'evento.

In virtù del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modificazioni, i log devono essere conservati in file su cui è possibile effettuare solo la scrittura incrementale o eventualmente su supporti non riscrivibili (es. CD-R). I log, opportunamente normalizzati e filtrati devono essere conservati su host dedicati. In ogni caso, deve essere possibile poter effettuare il backup dei log secondo le normali procedure di backup previste dalla Regione.

L'accesso ai log deve essere concesso al minor numero possibile di incaricati preventivamente individuati.

La frequenza di rotazione dei log è dipendente dalla frequenza di generazione degli eventi del sistema e da eventuali vincoli tecnici o legali. In ogni caso deve essere previsto un meccanismo che, successivamente al backup, sovrascriva i log esistenti ad intervalli regolari.

Ove possibile, gli amministratori devono mantenere on line i file di log contenenti gli eventi di sicurezza per almeno 1 mese.

I log devono essere conservati per un periodo di almeno 6 mesi ai sensi del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 e successive modificazioni. E'opportuno che la conservazione avvenga su supporto di memorizzazione offline non accessibile in scrittura ad alcuno.

Gestione degli incidenti di sicurezza

Tutti gli amministratori devono reagire agli incidenti di sicurezza con prontezza e con spirito di cooperazione, segnalando al proprio responsabile e alla direzione competente in materia di Sistemi Informativi le violazioni di sicurezza interna o gli eventi che possono portare a credere che vi sia stata un'elusione delle misure di sicurezza previste.

Gli amministratori, dopo una prima verifica dell'accaduto, devono registrare le operazioni svolte e contattare la direzione competente in materia di Sistemi Informativi.

Per gestire correttamente gli incidenti è indispensabile avere un elenco aggiornato dei beni (assets) che permetta di identificare i sistemi/applicazioni e il relativo livello di criticità.

Le macrofasi di gestione dell'incidente sono le seguenti:

- rilevazione incidente;
- identificazione e analisi dell'incidente;
- contenimento, raccolta evidenze, rimozione e ripristino;
- chiusura dell'incidente.

Le procedure dettagliate di gestione delle violazioni di sicurezza sono oggetto di apposito disciplinare tecnico sulla gestione dei data breach.

Controlli di sicurezza

Analisi dei rischi

E' obbligo di ogni amministratore valutare i potenziali rischi di sicurezza derivanti dal design, l'installazione, l'utilizzo e la gestione dei sistemi informatici di competenza.

Ogni progetto che prevede l'installazione, l'utilizzo, la modifica, l'eliminazione di uno o più sistemi informatici, deve quindi essere preceduto da un'adeguata analisi dei rischi che tenga conto del valore delle risorse da proteggere, delle potenziali minacce di sicurezza, dei meccanismi di sicurezza.

Security audit

I sistemi informatici sono periodicamente valutati ed analizzati per identificare il livello di rischio cui le risorse sono esposte.

Opportune verifiche sono regolarmente effettuate per valutare l'efficacia e l'efficienza dei meccanismi di sicurezza utilizzati.

I security audit possono essere affidati a fornitori esterni di servizi. In tal caso è necessario farsi rilasciare da questi ultimi apposita attestazione di conformità del servizio fornito ai requisiti previsti dalla normativa vigente in materia di protezione dei dati personali.

Documentazione tecnica

Gli amministratori di sistema hanno il compito di provvedere alla documentazione e al tempestivo aggiornamento della stessa, in relazione a tutti i sistemi, banche dati, apparati di rete e sicurezza, applicazioni software di qualunque natura e complessità, nonché alle procedure operative di installazione, configurazione ed aggiornamento delle strumentazioni informatiche e telematiche di competenza. Tale documentazione deve essere messa a disposizione in apposita sezione di Intranet ad accesso riservato per la consultazione sia da parte degli amministratori di sistema, sia da parte dei soggetti incaricati per quanto di propria competenza.