Disciplinare tecnico amministratori di sistema

Attuazione Provvedimento del garante nr.300/2008

Indice generale

1. Premessa

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; modificato con Provvedimento del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009), la definizione di "amministratori di sistema", ai fini dell'applicazione del presente disciplinare, è la seguente:

> **«amministratori di sistema»** 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.

Premesso che successivamente all'entrata in vigore del regolamento europeo 2016/679 sono stati approvati dalla Giunta regionale Toscana (nel seguito Ente) i seguenti documenti:

- Nomina del DPO, Deleghe del Titolare e Istruzioni agli autorizzati al trattamento dei dati personali (rif. Delibera nr. 585/2018 all.1)
- Data Protection Policy – Modello organizzativo (rif. Delibera nr. 521/2019)
- Data Protection Policy – Line guida (rif. Decreto dirigenziale nr. 7677/2019)
- Linee guida sulla sciurezza (in via di approvazione)

Considerato che il Regolamento (UE) n. 679/2016 non richiama espressamente gli amministratori di sistema, ma tali figure professionali continuano a trovare la propria disciplina nei Provvedimenti del Garante sopra citati, che non essendo in contrasto con la nuova normativa regolamentare europea rimangano pienamente vigenti ed efficaci; a ciò si aggiunge il riferimento implicito agli stessi nell'art. 32 del richiamato Regolamento, essendo tali professionalità quelle idonee allo svolgimento delle attività in esso contenute.

In particolare, l'art. 32, nella sezione "sicurezza dei dati personali", disciplina la sicurezza del trattamento. Le attività del punto 1 di cui alle lett. a) "cifratura e pseudonimizzazione dei dati"; b) "capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"; c) "capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico" e d) "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento" presuppongono la necessaria partecipazione di personale specialistico esperto nella gestione e nella trattazione informatica dei dati personali, con esperienza propria di amministratore di sistema, così come la necessità di un intervento tecnico di tali soggetti sin dalle fasi di progettazione e protezione dei dati (data Protection by design e by default).

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 e alle specifiche competenze in ambito Data Protection;
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 in relazione agli asset gestiti;
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 apposito elenco (rif. Allegato al presente documento). 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, l'Ente 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 l'Ente conserva, presso il security IT manager e il responsabile dell'infrastruttura ognuno per la parte di propria competenza, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche del fornitore 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 Security IT Manager, in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i direttamente gli asset gestiti e di riflesso i trattamenti dei dati personali previste dalle norme vigenti;
f) *registrazione degli accessi*: devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione) 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.
g) *formazione*: tutto il personale designato quale amministratore di sistema deve essere opportunamente aggiornato e formato relativamente agli aspetti sia operativi (in base al lavoro tecnico da svolgere) sia sugli aspetti inerenti la sicurezza delle informazioni. Il personale inoltre deve essere formato specificatamente sulle policy di sicurezza (fra cui la Data Protection Policy), procedure, e regolamenti emessi dall'Ente sia sui temi della Sicurezza delle informazioni sia più specificatamente su aspetti di Data Protection (reg. UE 679/2016)

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.

2. Applicabilità

Le regole illustrate nel disciplinare tecnico si applicano a tutti i dipendenti appartenenti all'organico dell'Ente e a tutti coloro che a vario titolo svolgono attività, compiti, mansioni come amministratori di sistema sotto la diretta responsabilità di dirigenti dell'ente.

3. Principi generali

Gli amministratori di sistema sono preposti alla sicurezza, alla gestione e alla manutenzione delle banche dati, dei sistemi e delle infrastrutture informatiche svolgendo attività tecniche al fine di garantire l'erogazione e la continuità dei servizi.

I principali processi in carico agli amministratori di sistema di norma sono:

- accertarsi e preoccuparsi che le infrastrutture di elaborazione siano installate in locali e spazi idonei ed adeguatamente protetti;
- gestire il sistema di asset management dell'ente che includa tutti gli apparati, i software, le banche dati e quant'altro sia necessario al corretto funzionamento dei sistemi informativi;
- impostare e gestire un sistema di autenticazione ed autorizzazione per l'accesso alle applicazioni e più in generale per l'accesso ai dati conforme ai regolamenti vigenti fra cui, in modo particolare, al reg. UE 679/16;
- assicurare e gestire sistemi di salvataggio e di ripristino dei dati e adottare procedure per la custodia delle copie di sicurezza;
- assicurarsi che le applicazioni siano sviluppate sempre secondo le policy e gli standard di sicurezza di Regione Toscana e che siano in linea con le principali buone prassi di riferimento;
- approntare adeguate misure e/o sistemi software di sicurezza per la salvaguardia dei dati e delle informazioni in conformità alle policy di sicurezza di Regione Toscana e ai regolamenti vigenti;
- organizzare la segmentazione e segregazione delle reti, la gestione dei supporti di memorizzazione,
- gestire la manutenzione di tutti i componenti hardware e software e delle contromisure di sicurezza,
- adottare un sistema idoneo alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici;
- gestire gli incidenti di sicurezza in collaborazione con il Security IT Manager nonché la verifica di eventuali tentativi di accessi non autorizzati al sistema;
- supportare il Security IT Manager e il DPO nelle attività di indagine e contrasto a potenziali Data Breach

- fornire a tutto il personale istruzioni organizzative e tecniche che prevedano le corrette modalità di utilizzo delle varie componenti dei sistemi informativi;
- Contribuire a predisporre con il Security IT Manager ed attuare un piano dei controlli periodici per verificare l'efficacia delle misure di sicurezza adottate;

È compito dell'amministratore di sistema monitorare costantemente lo stato di sicurezza e di efficacia di tutti i processi sopra descritti analizzando costantemente le minacce e le vulnerabilità di sicurezza incombenti sui propri sistemi e adottando (o rivedendo) le misure di sicurezza necessarie ad assicurare riservatezza, integrità e disponibilità dei dati e delle informazioni.

A titolo esemplificativo e non esaustivo 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).

4. Sicurezza fisica

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

La scelta dei locali in cui installare, conservare o utilizzare sistemi informatici è 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 sono valutate e adottate idonee misure di protezione, quali sistemi di controllo accessi, sistemi di protezione perimetrale, sistemi antintrusione, segregazione di aree critiche, chiusure di armadi contenenti Hardware, casseforti ignifughe per la conservazione di supporti removibili, ecc.

Gli amministratori di sistema possono essere chiamati a detenere e gestire le chiavi fisiche o le credenziali (pin, smart card) per l'accesso fisico sia ai locali contenenti le apparecchiature informatiche sia ad armadi e casseforti contenenti apparecchiature hardware (rete, server, storage, supporti removibili, ecc.).

I dispositivi di accesso fisico ai locali e/o apparati hardware consegnati agli amministratori di sistema sono strettamente personali e non cedibili e quando non utilizzate devono essere conservate dagli stessi in modo da non poter essere utilizzate da personale non autorizzato.

La consegna delle chiavi (o credenziali) per l'accesso fisico ai locali e/o apparati hardware devono essere tracciate in apposito registro non modificabile.

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 (D.Lgs. n. 81/2008, "Testo Unico sulla Sicurezza e Salute delle Lavoratrici e 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 di 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 inoltre sia presso le portinerie dell'Ente sia da parte di un eventuale custode specificatamente incaricato.

5. Controllo dell'accesso ai dati e ai sistemi da parte degli amministratori

L'accesso ai dati ed alle strumentazioni informatiche utilizzate per trattarli deve essere concesso al solo personale espressamente autorizzato ed individuato come amministratore di sistema. Nel caso in cui l'amministratore abbia accesso anche a dati personali è necessario che lo stesso sia indicato fra le persone autorizzate al trattamento all'interno dello stesso registro dei trattamenti.

In nessun modo devono essere concessi permessi di accesso ai sistemi senza preventivo aggiornamento della anagrafe degli amministratori di sistema e conseguente comunicazione al security manager. Le modalità tecniche attraverso le quali avviene l'aggiornamento e la comunicazione sono elementi da concordare fra il security manager e il Responsabile.

Gli Amministratori di sistema operano sotto il diretto controllo del Responsabile o del Titolare pertanto è specifica responsabilità di quest'ultimi provvedere al provisioning e soprattutto al tempestivo deprovisioning delle autorizzazioni all'accesso e a fissare regole di validità temporale di dette autorizzazioni.

5.1.1 Autenticazione

L'accesso ai dati trattati con strumentazioni informatiche deve avvenire esclusivamente previa opportuna autenticazione personale.

Gli strumenti di autenticazione devono essere progettati in funzione del valore dei dati trattati tenendo presente sia valore interno che può avere l'informazione per l'Ente sia valore esterno quale ad esempio il valore dell'informazione per l'interessato come nel caso dei dati personali. 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 (vedasi anche paragrafo 5.2), 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 di amministrazione.

1.2.1 Autorizzazione

È necessario che siano esplicitati nella comunicazione degli amministratori di sistema i ruoli amministrativi e i ruoli operativi degli stessi.

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).

Ogni credenziale di autenticazione deve riferirsi ad un singolo utente. Non è consentito l'utilizzo di credenziali condivise. Ove possibile, bisogna privilegiare sempre l'utilizzo di credenziali nominative anche nel caso di operazioni di amministrazione dei sistemi. Fanno al momento eccezione a queste regole le credenziali amministrative di accesso ai sistemi (es. root, administrator), che devono comunque essere assegnate ad un responsabile e devono essere utilizzate solo nel caso di interventi particolari sui sistemi che non è possibile effettuare attraverso delle credenziali nominative con i privilegi da amministratore. Il responsabile che detiene le credenziali di amministratore generiche di accesso ai sistemi (admin, root, ecc) dovrebbe non occuparsi di operare direttamente sui sistemi con tali credenziali ma bensì solo di assegnare tali credenziali agli specialisti che ne necessitano. L'attribuzione di tali credenziali generiche deve essere temporanea e loggata in apposito registro (cartaceo o digitale). Una volta terminata l'operatività dell'amministratore che ha operato sui sistemi la password di tale credenziale deve essere cambiata da parte del responsabile stesso. Possono essere utilizzate in alternative soluzioni software automatizzate PAM (Privileged Access Management) per garantire un corretto utilizzo delle credenziali di amministratore.

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 email: 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 email 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 email 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, ave possibile).

2. Gestione delle credenziali per l’accesso alle funzioni applicative da parte degli utenti

Le credenziali consentono all'utente di accedere a funzioni applicative di trattamento di 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.

Tale processo si identifica come provisioning e deprovisioning delle credenziali.

A Tale processo deve sovraintendere una funzione di amministratore di sistema sia che venga svolta da amministratori di sistema individuati dal Responsabile o dal Titolare nel caso in cui tale processo sia delegato attraverso specifiche funzioni applicative a personale indicato dal titolare stesso. In ogni caso il responsabile tiene traccia degli amministratori di sistema e delle loro azioni sui sistemi.

Le richieste agli amministratori di sistema delle credenziali di autenticazione da assegnare agli utenti, devono essere fatte esclusivamente dai Titolari dei trattamenti o da persone da loro espressamente delegate a tale funzione . In ogni caso, deve essere tenuta traccia della richiesta che ha generato la creazione di una credenziale di autenticazione e accesso all’applicazione. La persona cui viene abbinata una credenziale di accesso deve essere registrata nel registro dei trattamenti in relazione al trattamento e alla credenziale assegnata. Risulta opportuno che la registrazione sul registro dei trattamenti e l’accettazione da parte dell’utente, avvenga preventivamente alla comunicazione all’amministratore di sistema e la conseguente attivazione.

Il tempo che intercorre fra la richiesta di credenziali all’amministratore di sistema deputato a questa funzione e la loro attivazione deve essere un elemento esplicitato nei livelli di servizio garantiti dal Responsabile al Titolare.

Ogni credenziale di autenticazione deve riferirsi ad un singolo utente. Non è consentito l’utilizzo di credenziali condivise.

La gestione delle credenziali deve seguire le procedure documentate per i vari sistemi di autenticazione. Ogni credenziale deve avere una data di inizio e una data di fine, la policy di scadenza delle credenziali non utilizzate è normalmente di 60 giorni. A tale regola possono

essere apportate modifiche su richiesta esplicita del Titolare o del Security manager in relazione a particolare applicazioni.

Credenziali che indipendentemente da quanto richiesto come periodo di inattività non sono utilizzate per 180 giorni, viene chiesta conferma della loro validità al titolare che se non conferma entro 15 giorni saranno disabilitate.

Il deprovisioning di credenziali deve produrre un'automatica cancellazione della persona dagli autorizzati nel registro dei trattamenti

Le policy di gestione delle password devono essere allineate sui diversi sistemi e comunque conformi alle policy e linee guida di sicurezza di Regione Toscana relativamente alle misure di sicurezza.

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.

1.2.1 Gestione delle password

La lunghezza minima e la complessità delle password deve essere impostata secondo quanto previsto dalle policy di sicurezza di Regione Toscana e in linea con le buone prassi vigenti. Ove la tecnologia non lo consenta, la lunghezza e la complessità 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 "bruteforce" 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 e resettare 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 personali o comunque di rilevanza strategica, devono essere previsti sistemi di controllo delle password per consentire il solo utilizzo di password

"resistenti" ad attacchi "bruteforce". 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.

6. Protezione dei dati

6.1.1 Backup dei dati

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 (da definirsi in base al tipo di dato sottoposto a backup) devono essere effettuati controlli a campione (su un campione opportunamente numeroso) 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 di bordo" 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 ignifughe le cui chiavi sono conservate da personale identificato.

L'elenco del personale autorizzato all'accesso ai locali/casseforti contenenti le copie 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 dei tasks 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 al le 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 con accesso riservato per la consultazione sia da parte degli amministratori di sistema sia da parte dei soggetti incaricati per quanto di propria competenza.

1.3.1 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 da 7 a 35 e incide proporzionalmente sui tempi delle procedure;
- Formattazione "a basso livello" (LLF) dei dispositivi di tipo hard disk, laddove passibile, 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.

Qualora non sia possibile procedere alla cancellazione sicura dei dati o alla distruzione del supporto removibile è possibile archiviare temporaneamente i supporti contenenti le informazioni presso un’area di stoccaggio sicura situata all’interno del datacenter (in attesa di successiva distruzione secondo le modalità ai punti precedenti)

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

7. Protezione delle applicazioni

7.1.1 Design, sviluppo, deployment e gestione

Le applicazioni devono essere sviluppate dispiegate e gestite secondo gli standard tecnologi pubblicati in:

http://www.e.toscana.it./e-toscana/it/standard_tecnologici.wp

Gli standard di riferimento devono tener conto del principio della data protection by design e by default contenuto nell'art. 25 del Regolamento (ue) n. 679/2016.

Tale principio impone al Titolare il rispetto della privacy già in fase di progettazione e per impostazione predefinita. I destinatari del principio della privacy by design e by default sono il processo che comporta il trattamento di dati personali nel suo complesso e i relativi applicativi che lo compongono. Nella fase di progettazione e implementazione, gli applicativi devono essere impostati nel rispetto delle norme e dei principi che regolano il trattamento dei dati personali.

In altre parole, gli strumenti richiamati devono tener conto dei principi quali la minimizzazione, che impone che siano trattati soltanto i dati "adeguati, pertinenti e limitati" a quanto necessario rispetto alle finalità del trattamento e della limitazione delle finalità del trattamento, che impone che i trattamenti successivi non siano "incompatibili" rispetto alle finalità prestabilite.

La consegna di una applicazione da parte di uno sviluppatore deve essere corredata da opportuna "Scheda data protection" nella quale lo sviluppatore stesso fornisce evidenza dei trattamenti, delle tipologie di dati trattati, dei rischi, delle minacce prese in considerazione e delle contromisure attuate oltre ad indicare eventuali requisiti di sicurezza che ritine debbano essere posti in essere dal soggetto gestore dell'infrastruttura se diverso. Tale scheda data protection è visionata e validata dal security manager e accompagna l'applicazione attraverso il suo ciclo di vita con gli aggiornamenti necessari. L'amministratore di sistema deputato al deployment dell'applicazione sui sistemi verificherà la scheda Data Protection e la aggiornerà per la parte di propria competenza.

8. Protezione dei sistemi e delle reti

È compito di ogni amministratore mantenere un elenco aggiornato e completo delle risorse gestite. L'elenco degli asset deve contenere almeno:

- i riferimenti fisici e logici dell'apparato (nome e indirizzo di rete), la sua ubicazione fisica e i riferimenti relativi al backup (quando esistente);
- il responsabile interno all'organizzazione che ha in carico l'asset
- le versioni dell'hardware, del firmware e del sistema operativo (quando esistente);
- le funzioni e applicazioni principali oppure il ruolo all'interno dell'infrastruttura regionale;

Tutte le modifiche agli apparati di produzione devono seguire idonee procedure che saranno contenute in apposito disciplinare di Change Management.

Precedentemente alla progettazione, implementazione, installazione o gestione di un sistema Hardware e Software, 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.

8.1.1 Server

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

Policy generale

a. Hardware, sistemi operativi, servizi ed applicazioni installati devono essere conformi al contratto di fornitura e concordati con il direttore esecutivo del contratto
b. Tutte le patch/hot-fixes 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 dell'Ente, adeguatamente giustificate, documentate e riportate dagli amministratori al Direttore esecutivo del contratto e al security manager l 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.
c. Servizi non sicuri devono essere sostituiti da equivalenti oggetti sicuri, ove ciò sia possibile. Per esempio servizi con traffico in chiaro (telnet) devono essere sostituiti da servizi con traffico cifrato (SSH).
d. Relazioni di fiducia tra sistemi possono essere configurate solo per specifiche esigenze di servizio. Devono essere documentate dagli amministratori ed approvate dal Direttore esecutivo del contratto che valuterà se coinvolgere il security manager
e. 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.
f. l 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.
g. Tutti i server di produzione devono essere collegati ad un sistema di UPS (Uninterruptible Power Supplies) 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 del Direttore esecutivo del contratto e del security manager con accesso riservato per la consultazione sia da parte degli amministratori di sistema sia da parte dei soggetti incaricati per quanto di propria competenza.

1.4.1 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

a. Tutti i router dovrebbero usare TACACS+ oppure RADIUS 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.
b. La password di enable deve essere configurata utilizzando il meccanismo di "enable secret" che ne permette la cifratura sicura.
c. Disabilitare le seguenti funzioni:
   - lP directed broadcast
   - pacchetti in ingresso con indirizzi non validi come da RFC 1918
   - TCP small services
   - UDP small services
   - tutti i source routing
   - tutti i servizi web
   - Protocollo CDP o similari
d. Usare la community SNMP adottata dall'Ente e comunque diversa da public o private, oppure limitare l'accesso agli apparati impostando opportuni filtri.
e. Le regole di accesso devono essere aggiunte o modificate aderendo alle necessità dell'Ente.
f. l router devono avere un banner di login che notifichi a chi accede che l'apparato è proprietà dell'Ente e che l'accesso è consentito al solo personale autorizzato.
g. Gli apparati di rete devono essere inclusi nel sistema di gestione dei sistemi di produzione adottato dall'Ente e quindi censiti riportando i riferimenti dei responsabili tecnici.
h. Deve essere utilizzato il protocollo SSH per gestire i router e: solo dove non tecnicamente possibile usare un canale sicuro di trasmissione.

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.

1.5.1 Workstation

Gli amministratori dei client devono tener conto delle policy generali relative alle workstation e devono documentare qualsiasi eccezione a queste regole.

Policy generale

a. il software utilizzato sulle workstation deve essere associato ad una licenza, in accordo con le specifiche del fornitore/produttore;
b. le workstation assegnate al personale dell'Ente devono essere utilizzate solo per gli scopi designati;
c. è vietato installare hardware e software addizionale senza autorizzazione del Responsabile del Settore in accordo con il Settore Infrastrutture e Tecnologie

d. è vietato alterare o cancellare software o modificare configurazioni su una workstation dell'Ente senza autorizzazione da parte del Responsabile del Settore Infrastrutture e Tecnologie

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.

1.6.1 Dispositivi portatili

l dispositivi portatili seguono le stesse policy indicate per le workstation 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 personale (es matricola, codice fiscale, ecc.).

Policy generale

a. 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.
b. Tutti gli hard disk di portatili che contengono informazioni di tipo personale devono essere cifrati
c. l 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.

9. Protezione delle reti e delle comunicazioni

Le policy e le procedure relative alle connessioni Internet, alle comunicazioni, alla sicurezza perimetrale, alla Intranet, alla DMZ, alla VPN ed alle connessioni wireless sono quelle riportate di seguito:

https://intranetgiunta.regione.toscana.it/intranet/htm/aree_tematiche/privacy/in_regione/atti/direttive.shtml

http://www.e.toscana.it/e-toscana/it/standard_tecnologici.wp

10. 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 sicurezza (lettura e scrittura);
- Modifica di funzioni amministrative (es. la disabilitazione delle funzioni di Jogging, 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 lP, 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 "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; modificato con Provvedimento del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009), 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 dall'Ente.

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.

l log devono essere conservati per un periodo di almeno 6 mesi, in virtù del 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, modificato con Provvedimento del 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009). E' opportuno che la conservazione avvenga su supporto di memorizzazione offline non accessibile in scrittura ad alcuno.

11. Gestione degli incidenti di sicurezza

Tutti gli amministratori di sistema devono reagire agli incidenti di sicurezza con prontezza e con spirito di cooperazione segnalando al proprio al responsabile della sicurezza e questo al direttore esecutivo del contratto e al security manager 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 tenere traccia delle operazioni fatte e devono contattare il Security Manager per le valutazioni richieste dal GDPR per le comunicazioni al garante.

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, collegando questi ai trattamenti.

Le macro fasi di gestione dell'incidente sono le seguenti:

- Rilevazione incidente;
- Identificazione e analisi dell'incidente;
- Contenimento, Raccolta evidenze, Rimozione e Ripristino;
- Chiusura dell'incidente.

Qualora si sospetti che l'incidente possa aver interessato dei dati personali è necessario che gli amministratori di sistema agiscano conformemente alla Data Protection Policy e alle modalità e tempi contenuti all'interno della procedura di gestione dei Data Breach avvisando immediatamente il Security Manager e il DPO di tale evento.

Ulteriori dettagli per la gestione degli incidenti sono contenuti all'interno del framework della sicurezza.

12. Controlli di sicurezza

12.1.1 Analisi dei rischi

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

Ogni progetto che prevede l'installazione, l'utilizzo, la modifica, l'eliminazione di uno o più sistemi 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 attivati e possibili.

12.2.1 Security audit

l sistemi 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.

Gli amministratori di sistema sono chiamati a collaborare con gli Auditor al fine di consentire agli stessi di acquisire tutte le informazioni necessarie per valutare l'efficacia delle misure di sicurezza implementate.

Qualora i security audit siano effettuati da fornitori esterni è necessario che gli stessi audit siano effettuati in conformità ai requisiti previsti dalla normativa vigente in materia di protezione dei dati personali (Reg. UE n. 679/16).