Regione Toscana

Amministratori di sistema

– Disciplinare –

Attuazione Provvedimento del Garante nr.300/200

DATA PROTECTION OFFICER
GIUNTA REGIONALE TOSCANA

Indice

1 Scopo

Il presente documento ha l'obiettivo di regolare l'attività degli amministratori di sistema dell'ente, per tutti quei trattamenti/servizi con utilizzo di strumenti IT, di cui lo stesso opera come Titolare in completa autonomia operativa sia fornisce indicazioni quando, per i trattamenti/servizi di cui ha la titolarità, si avvale di un soggetto esterno, Responsabile, per la loro erogazione o gestione.
In quest'ultimo caso le indicazioni si basano sull'esigenza che anche il Responsabile disponga di un disciplinare tecnico per gli amministratori di sistema e che la loro organizzazione sia conosciuta al Titolare e che i processi di amministrazione delle componenti IT abbiano coerenza con le disposizioni che il Titolare adotta per analoghe funzioni.

2 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 o redatti i seguenti documenti:

1) Nomina del DPO, Deleghe del Titolare e Istruzioni agli autorizzati al trattamento dei dati personali (Regione Toscana rif. Delibera nr. 585/2018 all.1)
2) Data Protection Policy – Modello organizzativo (Regione Toscana rif. Delibera nr. 521/2019)
3) Data Protection Policy – Line guida (Regione Toscana rif. Decreto dirigenziale nr. 7677/2019)
4) Linee guida sulla sicurezza IT

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 digitale 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).

3 Applicabilità

Le regole illustrate nel presente disciplinare tecnico si applicano a tutto il personale appartenente all'organico del Titolare. Analogo disciplinare, in coerenza con il presente, è richiesto ai fornitori di servizi IT (Responsabili).

4 Principi generali

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) *La nomina degli "amministratori di sistema"* che operano sotto la diretta responsabilità del Titolare o del Responsabile avviene da parte delle

rispettive responsabilità organizzative. Per la Regione Toscana la nomina avviene da parte del dirigente della struttura cui compete la gestione del particolare Asset e tale nomina viene comunicata al Security IT Manager. Nel caso in cui per il trattamento dati sia stato individuato un Responsabile quest'ultimo comunica al Titolare Regione Toscana il nominativo del "responsabile della sicurezza IT" e i nominativi degli amministratori di sistema;

b) *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;
c) *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;
d) *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*, sia con proprie strutture sia avvalendosi di un soggetto esterno, l'Ente rende nota o conoscibile l'identità degli amministratori di sistema con comunicazione effettuata nell'ambito del portale di comunicazione interna, Intranet;
e) *servizi in outsourcing:* nel caso di servizi di amministrazione di sistema affidati in outsourcing l'Ente conserva, presso il Security IT manager o una articolazione organizzativa da lui individuata, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche del fornitore (Responsabile) preposte quali amministratori di sistema. Nel caso di un servizio di outsourcing il fornitore (outsourcer) nomina e comunica all'Ente, nelle persone del direttore esecutivo del contratto (DEC) e del Security IT Manager, il "responsabile della sicurezza IT", da cui dipendono gli amministratori di sistema;
f) *verifica delle attività:* l'operato degli amministratori di sistema, sia relativi a gestioni dirette sia attraverso fornitori esterni, 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 direttamente gli asset gestiti e di riflesso i trattamenti dei dati personali;
g) *registrazione degli accessi ai sistemi:* devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione) ai sistemi di elaborazione e agli archivi elettronici e alle altre componenti del sistema

informativo, 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, definito dal responsabile della sicurezza IT sulla base del valore dei dati acceduti, non inferiore comunque a sei mesi.

h) *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 alla sicurezza delle informazioni. Il personale inoltre deve essere formato specificatamente sulle policy di sicurezza (fra cui la Data Protection Policy, linee guida sulla sicurezza IT, ecc.), 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: (i) 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; (ii) per Asset, una componente tecnologica, virtuale o fisica, del sistema informativo. Sono Asset a cui applicare misure di sicurezza: (i) l'applicazione nel suo ciclo di vita, (ii) il sistema di autenticazione e autorizzazione (IAM), (iii) il dbms, (iv) il file server, (v) l'application server, (vi) il cms, (vii) la macchina virtuale, (viii) gli apparati di rete fisici o virtuali, (ix) i server, (x) le data storage, (xi)le workstation, ecc..

5 L'organizzazione

In sintesi, l'articolazione organizzativa entro la quale l'amministratore di sistema si trova ad operare, prevede:

1) Per la Giunta Regionale

a) *Il Titolare*: la Giunta;
b) *Delegato del titolare* (DGR.585/2018): dirigente della struttura competente relativamente al trattamento dati;
c) *Security IT Manager:* (DGR. 585/2018) Dirigente regionale preposto alla formulazione di indirizzi e verifica in merito alle misure di sicurezza IT;
d) *Comitato per la sicurezza IT:* Comitato presieduto dal Security Manager e composto dai Responsabili IT, con la partecipazione, quando richiesto, del DPO;
e) *Responsabile IT:* Dirigente responsabile dello sviluppo e gestione di Asset IT;
f) *Amministratore di sistema*: funzionario con competenze e conoscenze adeguate, individuato dal Responsabile IT per gli ambiti di competenza, che opera secondo gli indirizzi del Security IT Manager.

In sintesi l'amministratore di sistema: (i) risponde gerarchicamente al dirigente IT, responsabile degli asset amministrati, al quale è assegnato e a lui riferisce per tutte gli aspetti che riguardano le esigenze di provvedere al miglioramento delle misure di sicurezza; (ii) risponde per la congruenza delle proprie attività agli indirizzi sulla sicurezza, al Security Manager con il quale collabora per tutti gli aspetti riguardanti, l'analisi degli incidenti e gli altri aspetti di carattere trasversale. Il Security manager e i diversi responsabili IT operano e definiscono i piani per la sicurezza IT all'interno del Comitato per al sicurezza IT.

1) Per il Responsabile:

a) *Responsabile (processor):* Fornitore di servizi sulla base di un contratto e relativo DPA;
b) *Responsabile della sicurezza IT:* Dipendente del fornitore (Responsabile) incaricato dello sviluppo e gestione degli asset IT;
c) *Amministratore di sistema:* Dipendente del fornitore che opera sotto la responsabilità del Responsabile della sicurezza IT.

Il Responsabile è tenuto ad adottare e comunicare al Titolare, nelle figure del DEC e del Security IT Manager: (i) il nominativo del suo Responsabile della sicurezza IT, (ii) il disciplinare degli amministratori di sistema e (iii) l'elenco degli amministratori di sistema.
Il Titolare ha il compito (art. 24 del GDPR) di "…. Mettere in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento."
Pertanto è compito: (i) del Responsabile della sicurezza IT, per conto del Responsabile, garantire al Titolare, o suo delegato, l'adeguatezza delle misure di sicurezza IT e (ii) del responsabile della sicurezza IT, attraverso gli amministratori di sistema, di gestire al meglio, e secondo le indicazioni ricevute, le risorse tecnologiche amministrate.
I rapporti in merito alla sicurezza IT, fra Titolare (Giunta Regionale) e Responsabile, sono tenuti rispettivamente dal Security IT Manager e dal responsabile della sicurezza IT.

6 I compiti

Gli amministratori di sistema, nell'ambito delle loro funzioni e del loro ruolo, sono preposti ad attività finalizzate a garantire la sicurezza, la gestione e la manutenzione delle applicazioni, delle banche dati, dei sistemi e delle infrastrutture tecnologiche, svolgendo attività tecniche al fine di assicurare l'erogazione e la continuità dei servizi in sicurezza, sulla base del presente disciplinare, delle indicazioni ricevute, dei mezzi e degli strumenti a disposizione.
Rimane in carico al Titolare o Responsabile, la responsabilità, a noma del GDPR, in merito alle misure tecniche organizzative adottate. Al Titolare spetta, inoltre, l'attività di indirizzo e controllo sulla corretta esecuzione da

parte del Responsabile, a quest'ultimo l'indirizzo e controllo di eventuali altri Responsabili (sub-responsabili).
I principali processi in carico agli amministratori di sistema, dipendenti del Titolare, sono:

1) Verificare che le infrastrutture di elaborazione siano aderenti alle misure di sicurezza prescritte dal Comitato per la sicurezza IT, così come siano le loro condizioni ambientali; è loro compito segnalare al Security IT Manager eventuali carenze e relativi impatti sulla sicurezza dei dati e continuità dei servizi, suggerendo, laddove possibile, opportuni rimedi e se nelle sue possibilità intervenire minimizzando i rischi; aggiornare al continuo il sistema di asset management che includa tutti gli apparati, i software, le banche dati e quant'altro sia necessario al corretto funzionamento dei sistemi informativi;
2) Gestire, se asset di sua competenza, il sistema di autenticazione e 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; gestire i sistemi di salvataggio e di ripristino dei dati, adottare ed eseguire procedure per la custodia delle copie di sicurezza;
3) Attuare, secondo le procedure indicate, il processo di deployment delle applicazioni assicurandosi che le stesse siano corredate di tutta la documentazione richiesta, compresa quella attestante che le applicazioni siano sviluppate secondo le policy e gli standard di sicurezza del Titolare e che siano in linea con le principali buone prassi di riferimento;
4) Mettere in atto le misure e/o sistemi software di sicurezza per la salvaguardia dei dati e delle informazioni in conformità alle policy di sicurezza del Titolare e ai regolamenti vigenti, verificandone l'adeguatezza nel tempo e segnalando al Responsabile IT eventuali nuove esigenze;
5) Assicurare, nell'esercizio delle sue attività di collocazione e configurazione dei sistemi, la segmentazione e segregazione delle reti, fisiche e logiche, la gestione dei sistemi di memorizzazione;
6) Gestire la manutenzione di tutti i componenti hardware e software e delle contromisure di sicurezza;
7) Gestire e verificare il corretto funzionamento delle registrazioni secondo le specifiche, del sistema di gestione degli accessi logici alle applicazioni, ai sistemi e agli archivi;
8) Gestire gli incidenti di sicurezza in collaborazione con il Security IT Manager nonché la verifica di eventuali tentativi di accessi non autorizzati al sistema;
9) Supportare il Security IT Manager e il DPO nelle attività di indagine e contrasto a potenziali Data Breach;
10) Collaborare attivamente in tutte le attività di audit;
11) Nell'attività di gestione delle risorse IT, affidate all'amministratore di sistema, è compresa l'attività proattiva e tempestiva nel segnalare

eventuali problematiche, suggerire soluzioni, mettere in atto misure tese a ridurre i rischi, gestire le emergenze con ampi gradi di libertà, responsabilità e professionalità, ecc..;

12) È compito dell'amministratore di sistema, nell'ambito delle dotazioni strumentali e tecniche messe a disposizione, 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, rivedendo e suggerendo le misure di sicurezza necessarie ad assicurare riservatezza, integrità e disponibilità dei dati e delle informazioni, anche alla luce degli incidenti occorsi o dei tentativi di intrusione sventati;
13) 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).

Ulteriori funzioni assegnate agli amministratori di sistema devono essere censiti a cura del responsabile della sicurezza IT.

7 Sicurezza fisica

La scelta dei locali in cui installare, conservare o utilizzare sistemi IT è fatta: dal Titolare, nella figura del Security IT Manager, o dal Responsabile, 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..

La scelta delle misure di sicurezza dei locali, spetta al Titolare, (per la Giunta al Security IT Manager), o al Responsabile, e 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.
L'accesso fisico ai locali è regolato dall'apposito disciplinare predisposto dal Titolare (nel caso della giunta dal Security IT Manager) o dal Responsabile.
Gli amministratori di sistema possono essere chiamati, da parte del Security IT Manager (nel caso della Giunta) o dal Responsabile della sicurezza IT, nel caso del Responsabile, a detenere e gestire le chiavi fisiche o le credenziali (pin, smart card) per l’accesso fisico sia ai locali, contenenti le apparecchiature ICT, sia ad armadi e casseforti contenenti apparecchiature hardware (rete, server, storage, supporti removibili, ecc.).
La consegna delle chiavi per l’accesso fisico ai locali e/o armadi contenenti apparati hardware devono essere tracciate in apposito registro, non modificabile, tenuto dal responsabile della sicurezza IT.
I dispositivi di accesso fisico sono strettamente personali e non cedibili e quando non utilizzati devono essere conservati, in modo da non poter essere utilizzati da altro personale.

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

L'accesso diretto ai dati ed alle strumentazioni IT, utilizzati nei trattamenti, deve essere concesso al solo personale espressamente individuato come amministratore di sistema.
Nel caso in cui l’amministratore effettui anche dei trattamenti di 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 dell’elenco degli amministratori di sistema e conseguenti comunicazioni. Qualora le attività di Amministrazione di sistema fossero svolte da altro soggetto (Responsabile), quest’ultimo si accorderà con il Security IT Manager dell’Ente, per la condivisione dell’elenco aggiornato degli amministratori di sistema.
Gli Amministratori di sistema operano per conto del Titolare o del Responsabile e pertanto è specifica responsabilità di quest’ultimi (per la Giunta Regionale il Security IT Manager) provvedere al provisioning e soprattutto al tempestivo deprovisioning delle autorizzazioni all’accesso e a fissare regole di validità temporale di dette autorizzazioni.

8.1 Autenticazione

L'accesso ai dati trattati con strumentazioni IT, 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 il 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 sia a livello di sistema operativo sia a livello applicativo, per consentire l'accesso ai dati e alle operazioni effettuate sugli stessi, in misura corrispondente ai diversi profili di amministrazione.

8.2 Autorizzazione

È necessario che siano esplicitati nella comunicazione degli amministratori di sistema (vedi Elenco) i ruoli amministrativi e i ruoli operativi degli stessi.
Il principio generale a cui attenersi è che i ruoli critici non si devono sovrapporre: pertanto i ruoli debbono essere assegnati in modo da garantire adeguati livelli di separazione delle funzioni più critiche, evitando ad esempio che una singola persona possa auto assegnarsi delle funzioni e svolgere attività di controllo su sé stessa, garantendo così un adeguato livello di controllo.
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.
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.
Pertanto sono da privilegiare strumenti che consentano tali opzioni come le soluzioni software PAM (Privileged Access Management).
Qualora non fosse possibile, rimane di responsabilità del Security IT Manager, o suo delegato, per la Giunta, o del Responsabile della sicurezza IT, nel caso del Responsabile, conservare tali credenziali, assegnarle alle persone, provvedere al loro periodico aggiornamento, garantendo in ogni momento e in maniera certa di poter risalire dall'operazione alla persona che effettivamente l'ha svolta.
Le credenziali amministrative non nominative, create al solo scopo di avviare servizi sui server devono essere disabilitate finito lo scopo e devono rimanere attive solo per il tempo strettamente necessario.
Le credenziali di autenticazione con privilegi amministrativi non devono essere inviate via email: in tali casi, è necessario convocare la persona e fornirgli le credenziali verbalmente, qualora non fosse possibile è nella responsabilità del Security IT Manager (per il Titolare Giunta) o del

responsabile della sicurezza IT, per il Responsabile, individuare il sistema maggiormente idoneo.
Gli amministratori dei sistemi sono tenuti a rispettare le procedure adottate e a non creare particolarità o eccezioni nella gestione delle credenziali utente, salvo per motivate necessità che debbano essere portate all'attenzione del Security IT Manager (Giunta) o del responsabile della sicurezza IT (Responsabile).
La gestione delle credenziali amministrative deve seguire regole molto rigide e stringenti sotto la supervisione del Security IT Manager (Giunta) o del responsabile della sicurezza IT (Responsabile).

9 Messa in esercizio di applicazioni

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.
La consegna di una applicazione da parte di uno sviluppatore per la messa in test o in produzione 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 ritiene debbano essere posti in essere dal soggetto gestore dell'infrastruttura se diverso. Tale scheda Data Protection è visionata e validata dal Security IT 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, verificherà le misure di sicurezza adottate nello sviluppo e definirà quelle aggiuntive da porre in essere a livello di infrastrutture o ambienti SW di base e la aggiornerà per la parte di propria competenza e ne garantirà l'aggiornamento nel tempo. Qualora nelle verifiche delle misure di sicurezza adottate riscontrasse delle incongruenze rispetto alle istruzioni ricevute, le segnalerà al proprio responsabile.

9.1 Gestione delle credenziali per l'accesso alle funzioni applicative da parte degli utenti

Le richieste agli amministratori di sistema delle credenziali di autenticazione da assegnare agli utenti, seguono il processo descritto delle linee guida sulla sicurezza IT dell'ente titolare.
Fra i "ruoli di amministrazione" deve esisterne uno specifico dedicato alla gestione delle utenze.

10 Apparati

10.1 Server

Per le modalità operative di installazione, configurazione, aggiornamento e gestione si rimanda alle valutazioni e alle specifiche definite del responsabile della sicurezza.
Tali modalità devono essere documentate, mantenute aggiornate, e messe a disposizione all'interno del processo di accountability definito nel documento Data Protection Policy della Regione Toscana (DGR521/2019 e DD 7677/2019).
In particolare, durante l'attività di configurazione e gestione dei sistemi server, l'amministratore dovrebbe garantire:

a. Hardware, sistemi operativi, midlle-ware ed applicazioni installati siano conformi a quanto dichiarato. 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 valutate. l servizi non necessari devono essere rimossi/disabilitati, compatibilmente con le dipendenze del sistema in oggetto. È compito degli amministratori di sistema mantenersi costantemente aggiornati sulle patches/hotfixes da installare. Servizi "non sicuri" o vulnerabilità conosciute devono essere segnalate e risolte nel più breve tempo possibile;
b. Eventuali relazioni di fiducia tra sistemi debbono essere progettate, comunicate all'amministratore di sistema in tempi tale da non creare ritardi in fase di implementazione e configurate solo per specifiche esigenze di servizio;
c. 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;
d. Devono sempre essere controllate le condizioni fisiche, ambientali al fine di garantire la continuità del servizio, eventuali problemi debbono essere prontamente comunicati, in modo che chi di competenza possa prontamente intervenire.

10.2 Apparati di rete

Per apparati di rete si intende: Router, Firewall, ecc.. sia che siano apparati fisici o virtuali.
Per le modalità operative di installazione, configurazione, gestione e aggiornamento, si rimanda alle valutazioni e specifiche definite in appositi documenti del responsabile della sicurezza e al documento linee guida sulla sicurezza e successive modifiche o integrazioni.
Le eventuali "isole" che concorrano alla formazione dell'architettura di rete debbono essere ben descritte all'interno della documentazione tecnica in modo da poter disporre di una visione generale dell'ambiente IT.
Gli amministratori di rete dovrebbero, ad esempio, garantire che:

a. L’ambiente IT sia definito e ben documentato;
b. Tutti i router usino TACACS+ oppure RADIUS per autenticare gli utenti o altro sistema a più alto livello di sicurezza;
c. L'accesso con account locali è consentito solo in situazioni d'emergenza ovvero quando non fosse disponibile il sistema centralizzato di autenticazione;
d. La password di “enable” deve essere configurata utilizzando il meccanismo di "enable secret" che ne permette la cifratura sicura;
e. Siano disabilitate 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 non necessari e/o non sicuri ,
   - Protocollo CDP o similari.
f. Si usi la community SNMP adottata dall'Ente e comunque diversa da public o private, oppure limitare l'accesso agli apparati impostando opportuni filtri.
g. Le regole di transito devono essere create, modificate ed espressamente documentate ivi comprese le relative motivazioni.
h. Le regole di accesso da parte degli amministratori devono essere documentate;
i. I 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.
j. Gli apparati di rete devono essere inclusi nel sistema di gestione dei sistemi di produzione e quindi censiti riportando i riferimenti dei responsabili tecnici.
k. Deve essere utilizzato il protocollo SSH per gestire i router e: solo dove non tecnicamente possibile usare un canale sicuro di trasmissione.
l. Quanto altro sarà definito da parte del Titolare o del Responsabile in appositi documenti di indirizzo.

Il responsabile della sicurezza IT deve produrre uno specifico documento di indirizzo per gli amministratori di sistema che individui le “garanzie di sicurezza” che debbono essere osservate.
Le modalità operative di installazione, configurazione ed aggiornamento, come pure gli schemi dell’ambiente IT, debbono essere documentati, mantenuti aggiornati, e messi a disposizione all’interno di un processo di accountability.

10.3 Workstation e dispositivi portatili

Per le attività di installazione, configurazione e aggiornamento si rimanda alle valutazioni e alle specifiche definite dal responsabile della sicurezza.
Gli amministratori delle workstation, dovrebbero ad esempio garantire che:

a. il software utilizzato sulle workstation, se associato ad una licenza deve averla, in accordo con le specifiche del fornitore/produttore;
b. le workstation assegnate al personale devono disporre di meccanismi per poter 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 competente;
d. è vietato alterare o cancellare software o modificare configurazioni su una workstation dell'Ente senza autorizzazione da parte del Responsabile del Settore competente.

I 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.).

Gli amministratori di sistema dovrebbero garantire che:

a. L’accesso alle impostazioni di sistema sia limitato (ad esempio, la password di accesso al BIOS su tutti i dispositivi sia impostata e non conoscibile all’utente finale; il boot da supporto rimovibile sia disabilitato da BIOS, …);
b. Se il firmware consente di proteggere con password l'hard disk, e se lo si ritiene necessario per casi particolari e documentati, sia abilitata anche questa funzionalità;
c. La medesima password per BIOS e hard disk deve essere utilizzata su tutti i dispositivi, per accelerare gli interventi tecnici approvati;
d. Tutti gli hard disk di portatili che contengono dati personali particolari o giudiziari o che si riferiscono a categorie particolari di interessati devono essere cifrati; in questa decisione concorre la valutazione del “valore del dato” e dei relativi rischi;
e. L’installazione e la verifica nel tempo che il software presente sia solo quello autorizzato;
f. Ogni altra condizione o regola che definisca l’utilizzo da parte delle stazioni di lavoro da parte del Personale;

Il Security IT Manager o il responsabile della sicurezza IT del fornitore debbono produrre un documento di indirizzo per gli amministratori delle work station e dei dispositivi portatili, atto a fornire adeguate “garanzie di sicurezza”.

E’ da valutare l’esigenza di avere profili di software differenziato. Per questo aspetto si faccia riferimento al documento PR-SGSI-09_Procedura

Gestione del Software Autorizzato delle linee guida sulla sicurezza, alle successive modifiche o integrazioni e alle valutazioni e specifiche definite dal responsabile della sicurezza.
Le modalità operative di installazione, configurazione ed aggiornamento, debbono essere documentate, mantenute aggiornate, e messe a disposizione all'interno del processo di accountability.

11 Backup dei dati

Per le procedure e le operazioni di Backup si rimanda alla valutazione e alle specifiche definite dal responsabile della sicurezza e alle linee guida sulla sicurezza e successive modifiche o integrazioni.
Al fine di garantire la disponibilità dei dati, l'amministratore dovrebbe prevedere 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.
Gli amministratori dovrebbero ad esempio garantire che:

a. 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;
b. 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;
c. 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;
d. 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;
e. L'elenco del personale autorizzato all'accesso ai locali/casseforti contenenti le copie deve essere regolarmente mantenuto aggiornato;
f. 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;
g. Gli amministratori del sistema di backup devono monitorare l'esito dei task eseguiti e, qualora rilevassero problemi, darne pronta segnalazione agli amministratori dei sistemi coinvolti;
h. 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.

Il Security IT Manager o il responsabile della sicurezza IT del fornitore debbono produrre un documento di indirizzo per gli amministratori, atto a fornire adeguate "garanzie di sicurezza" che tengano conto del "valore del dato personale" trattato.

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.

12 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.
Per questo aspetto si rimanda alle valutazioni e alle specifiche definite dal responsabile della sicurezza e al documen delle linee guida sulla sicurezza e successive modifiche o integrazioni
La definizione ed il rilevamento degli eventi di sistema devono essere effettuati in funzione del "valore dei dati" ed in modo tale da consentire la verifica dell'efficacia e dell'efficienza delle procedure di sicurezza. Ad esempio, ove possibile dovrebbero essere rilevati:

- Autenticazione (login e logout, riusciti e non);
- Accesso ai Dati Personali in funzione del loro valore (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 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 un periodo minimo definito in base alle specifiche del Responsabile della Sicurezza che tenga conto del valore dei dati trattati.
l log devono essere conservati per un periodo di almeno 6 mesi, periodi più lunghi saranno valutati in relazione al valore del dato, 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 non accessibile in scrittura ad alcuno, eventualmente anche offline, se Offline occorre definire il tempo di mantenimento, finito il quale si deve procedere alla distruzione dei log.

13 Procedure di dismissione dei sistemi

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.
Per questo aspetto si rimanda alle valutazioni e alle specifiche definite dal Responsabile della Sicurezza.
Le modalità di dismissione dei sistemi debbono essere documentate, mantenute aggiornate, e messe a disposizione all’interno del processo di accountability.
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, adeguatamente individuata con adeguate garanzie di sicurezza.
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.

14 Gestione degli asset

La gestione degli asset è descritta nel documento PR-SGSI-18_Procedura del ciclo di vita degli Asset delle linee guida sulla sicurezza IT, e successivi aggiornamenti o integrazioni.
È compito di ogni amministratore di sistema mantenere un elenco aggiornato e completo delle risorse gestite in quanto a lui assegnate. 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.

Tutti gli interventi tecnici che coinvolgono la creazione, modifica o eliminazione di uno dei meccanismi di sicurezza messi in campo, devono essere opportunamente documentati ed autorizzati da parte del proprio responsabile.

15 Controlli di sicurezza

15.1 Analisi dei rischi

E' obbligo di ogni amministratore di sistema valutare i potenziali rischi di sicurezza derivanti dal design, dall'installazione, dall'utilizzo e dalla gestione degli Asset di competenza a lui assegnati, opera in questo in team con il responsabile della sicurezza IT e gli altri amministratori di sistema.
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. Questo deve andare a formare uno specifico documento che accompagna l’intervento sistemistico.

15.2 Security audit

I sistemi sono periodicamente valutati ed analizzati (audit Interno) per identificare il livello di rischio cui le risorse sono esposte. Inoltre opportune verifiche sono regolarmente effettuate per valutare l'efficacia e l'efficienza dei meccanismi di sicurezza utilizzati. Per tale aspetto si fa riferimento al documento PR-15-Procedure di security Audit delle linee guida per la sicurezza e sue successive modifiche ed integrazioni.
Eventuali anomalie sono tempestivamente comunicate dall’amministratore di sistema al suo responsabile che attiverà la procedura di incident management.
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.

15.3 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 responsabile le violazioni di sicurezza interna o gli eventi che

possono portare a credere che vi sia stata un'elusione delle misure di sicurezza previste.
Per quanto riguarda tale problematica si fa riferimento alla Data Protection Policy della Regione Toscana e alle linee guida sulla sicurezza IT e successive modifiche e integrazioni.
Gli amministratori, dopo una prima verifica dell'accaduto, devono tenere traccia delle operazioni fatte e devono contattare il Security IT Manager del Titolare per le valutazioni richieste dal GDPR e per le comunicazioni al Garante.
Per gestire correttamente gli incidenti è indispensabile avere un Catalogo degli Asset che permetta di identificare i sistemi/applicazioni e il relativo livello di criticità, collegando questi ai trattamenti (vedi Data Protection Policy Regione Toscana).

16 Allegato: formato elenco amministratori di sistema e relativa nomina.

L’elenco degli amministratori di sistema deve individuare, oltre ai suoi elementi identificativi, l’ambito tecnico di responsabilità e i privilegi.
L’ambito tecnico di responsabilità si evidenzia attraverso gli asset di cui l’amministratore garantisce la gestione e relativi livelli di sicurezza oltre al rilevamento di incidenti e loro comunicazione.
L’elenco è predisposto e tenuto aggiornato dal responsabile della sicurezza. Riguarda si agli Enti nella veste di Titolare sia altri soggetti nella loro veste di Responsabili.
L’attribuzione della funzione di amministratore deve essere formale e sottoscritta per accettazione e per presa visione dei suoi compiti generali, descritti nel disciplinare degli amministratori di sistema, e specifici derivanti da istruzioni che il Titolare o il Responsabile intende definire.

16.1 Esempio Struttura elenco amministratori di sistema.

A titolo esemplificativo:

Cognome e Nome	Asset di riferimento	Titolare dei dati contenuti negli asset	Privilegi	Data Inizio-Data Fine	Note

16.2 Esempio di nomina/ordine di servizio per amministrazione di sistema.

Ente/Fornitore: _____
Ordine di servizio: Nomina ad Amministratore di Sistema.
Il Sig./sig.ra ***Nome e Cognome***, che dispone delle adeguate conoscenze, è nominato/a Amministratore di Sistema, a norma del Regolamento Europeo 679/2016 (GDPR) e Decreto Lgs. 196/2003 (codice in materia di protezione dei dati personali), dalla data _____ alla data _____ in relazione ai seguenti Asset e relativi privilegi:

Asset	Titolare dati	Privilegi
_____	_____	_____
_____	_____	_____
_____	_____	_____

Nell'esercizio della sua attività è chiamato e si impegna: al pieno rispetto della normativa in materia di protezione dei dati personali e dei principi di riservatezza che ne derivano, a conformare il proprio comportamento, nell'esercizio delle sue funzioni, al disciplinare degli amministratori di sistemi e agli altri documenti di indirizzo o linee guida in merito alla Protezione dei Dati, prodotti e messi a sua conoscenza da parte del Titolare o suo delegato per la sicurezza IT.

Il Titolare/Responsabile. F.to _____

La persona incaricata F.to _____