DISCIPLINARE TECNICO PER AMMINISTRATORE DI SISTEMA

DOCUMENTO	DATA EMISSIONE	VERIFICATO DA	APPROVATO DA
5.3.1DOC_01	13/05/19	consiglio direttivo	presidente

FIRMATO	
presidente	

REGISTRAZIONE DELLE MODIFICHE

REVISIONE	DATA	SEZIONE	DESCRIZIONE
0.0			prima emissione

INDICE

0.0 SCOPO DEL DOCUMENTO

Il Disciplinare tecnico per amministratori di sistema viene redatto in attuazione 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, al fine di:

- descrivere le basilari regole tecniche ed organizzative che gli amministratori di sistema devono applicare per garantire la sicurezza dei dati e delle informazioni trattate con l’utilizzo di strumentazioni informatiche
- regolamentare le attività degli amministratori amministratori di sistema
- proteggere i dati personali e le informazioni contro i rischi di distruzione, perdita e accesso non consentito

0.1 RESPONSABILITÀ

TITOLARE DEL TRATTAMENTO (TDT)
E il soggetto che, esercitando un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ha il compito di conciliare l’esigenza di tutela della privacy del personale (Responsabili, Incaricati e Amministratori di Sistema) ed il corrispondente potere/dovere del assicurare la funzionalità e il corretto impiego degli strumenti informatici.

AMMINISTRATORE DI SISTEMA (ADS)
figura professionale individuata dal titolare del trattamento, finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti

0.2 CAMPO DI APPLICAZIONE

Le regole illustrate nel presente documento si applicano a tutti i soggetti che svolgono mansioni, compiti ed attività in qualità di amministratori di sistema.

0.3 RIFERIMENTI NORMATIVI E DOCUMENTALI

RIFERIMENTI NORMATIVI	• Regolamento UE 2016/679 • Provvedimento del Garante Privacy del 27.11.2007 “Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema”
DOCUMENTI	• Manuale Organizzativo Privacy – sez 5.3.1 • Procedura di gestione dell'amministratore di sistema (doc. 5.3.3PRD) • Disposizioni generali per il trattamento dei dati personali e l'utilizzo degli strumenti elettronici • Disciplinare in materia di utilizzo degli strumenti informatici

I documenti disponibili in formato elettronico sono reperibili nella cartella PRIVACY delle risorse di rete condivise

0.5 DEFINIZIONI

AMMINISTRATORE DI SISTEMA	figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché 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.
ACCESS LOG	registrazione degli eventi generati dal sistema di autenticazione informatica all'atto dell'accesso o tentativo di accesso da parte di un amministratore di sistema o all'atto della sua disconnessione nell'ambito di collegamenti interattivi a sistemi di elaborazione o a sistemi software

POSTA ELETTRONICA	messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza
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.
COMUNICAZIONE ELETTRONICA	ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico
STRUMENTI ELETTRONICI	gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento

1 DISCIPLINARE TECNICO PER AMMINISTRATORI DI SISTEMA

1.1 PREMESSA

Gli amministratori di sistema sono soggetti che, nella definizione normativa, 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 di fatto responsabili di specifiche operazioni che possono comportare elevate criticità rispetto alla protezione dei dati personali.

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:

- 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.
- 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.
- elenco degli amministratori di sistema: sono registrati gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite
- 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'organizzazione rende nota al personale l'identità degli amministratori di sistema
- nel caso di servizi di amministrazione di sistema affidati in outsourcing l'organizzazione conserva gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema
- verifica delle attività: l'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del Titolare del trattamento
- sono adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le

registrazioni (*access log*) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

1.2 COMPITI GENERALI DELL'AMMINISTRATORE DI SISTEMA

L'amministratore di sistema ha il compito di comprendere le minacce di sicurezza incombenti sui sistemi e adottare le misure necessarie ad assicurare che i dati e le informazioni siano riservati, integri e disponibili, proteggendoli dai rischi di distruzione, perdita ed accesso non consentito.

Deve attenersi scrupolosamente a tutte le procedure operative e segnalare immediatamente al Titolare o Responsabile del trattamento qualsiasi evento o situazione, anche solamente sospetta, che possa compromettere il buon funzionamento del sistema informativo.

Le mansioni e le responsabilità sono analiticamente individuate nella lettera di nomina

AMMINISTRATORI DI SISTEMA ESTERNI

Gli Amministratori di Sistema esterni o i tecnici e consulenti di società terze possono collegarsi alla rete informatica direttamente con i propri dispositivi, solo con la supervisione del Titolare, del Responsabile o dell'Amministratore di sistema interno.

Gli Amministratori di Sistema esterni, al completamento dell'attività, devono produrre un documento che attesti la data e ora di inizio e fine intervento e il dettaglio dell'attività svolta

1.3. SICUREZZA FISICA DEI SISTEMI SERVER E DI RETE

L'amministratore di sistema verifica che i locali in cui sono installati, conservati ed utilizzati i sistemi informatici siano:

- protetti contro potenziali rischi di sicurezza, accidentali o dolosi, adottando idonee misure di protezione, quali sistemi di anti-intrusione, sistemi anti-incendio, sistemi di rilevazione fumi, sistemi anti-allagamento.
- conformi ai vincoli imposti dalla normativa in materia di tutela della salute e di sicurezza dei lavoratori (D.Lgs. 81/2008)
- ad accesso limitato ed idonei e possibilmente dedicati all'esclusivo collocamento dei sistemi
- muniti di sistemi di condizionamento dell'aria nei locali per garantire il mantenimento di una costante ed adeguata temperatura ed umidità di esercizio

I sistemi, server ed apparati di rete considerati critici per il funzionamento e la disponibilità dei sistemi informativi, devono essere:

- muniti di sistemi di protezione elettrica, quali stabilizzatori di corrente ed apparecchiature UPS che consentano una disconnessione (*shutdown*) automatica dei server prima dell'esaurimento delle batterie.
- collocati in armadi chiusi a chiave e classificati con il giusto grado di protezione, in relazione all'ambiente in cui sono collocati

1.4. ACCESSO AI DATI

L'accesso ai dati ed agli strumenti elettronici impiegati per il loro trattamento è consentito al solo personale autorizzato, formalmente incaricato. L'organizzazione, per disciplinare l'accesso ai dati, adotta la *Procedura di gestione del sistema di autenticazione e autorizzazione.*

1.4.1 SISTEMA DI AUTENTICAZIONE

L'accesso ai dati trattati con strumenti elettronici deve essere concesso esclusivamente previa opportuna autenticazione informatica. Possono essere impiegati diversi sistemi di autenticazione, quali le credenziali informatiche costituite dalla coppia di nome utente e password, oppure, nel caso di trattamento di dati ed informazioni particolarmente riservate, strumenti quali *smart card*, *token* hardware, dispositivi *one-time password*, sistemi biometrici, ecc.

Devono essere previsti diversi tipi di autenticazione in relazione ai differenti domini applicativi ai quali deve essere consentito l'accesso (risorse di rete, applicativi software, banche dati intranet o internet ecc.).

Ad ogni *login* amministrativo deve corrispondere un *logout* anche nel caso di assenza temporanea

1.4.2 SISTEMA DI AUTORIZZAZIONE

Il sistema di autorizzazione circoscrive e definisce l'acceso alle tipologie di banche dati informatiche ai quali gli Incaricati possono accedere, quando per Incaricati sono individuati profili di autorizzazione di ambito diverso. I sistemi devono gestire l'accesso alle risorse informatiche associando le credenziali di autenticazione ad un profilo di autorizzazione.

L'accesso alle risorse di rete deve essere gestito per gruppi di lavoro, ed ogni Incaricato deve avere accesso selettivo alle cartelle del gruppo di lavoro di appartenenza, impostando . Il profilo di autorizzazione è generalmente impostato per classi omogenee di incaricati.

1.4.3 GESTIONE DELLE CREDENZIALI DI AUTENTICAZIONE

L'amministratore di sistema è responsabile della corretta applicazione delle politiche di gestione delle credenziali di autenticazione e si attiene a quanto specificato nella *Procedura di gestione del sistema di autenticazione e autorizzazione* adottato dall'organizzazione.

1.4.4 GESTIONE DELLE CREDENZIALI DI AMMINISTRAZIONE

Sebbene le credenziali di accesso nella gestione amministrativa dei sistemi (es. *root*, *administrator*) non sono nominative ed il loro utilizzo non è vincolato dalle norme applicabili alle credenziali di accesso degli incaricati, occorre comunque:

- privilegiare l'utilizzo di credenziali nominative anche nel caso di operazione di amministrazione
- assegnare le credenziali ad un numero limitato di incaricati
- utilizzare solo nel caso di necessari interventi di amministrazione sui sistemi.
- adottare politiche manuali di modifica delle password dei loro sistemi e a monitorare gli eventuali tentativi di accesso non autorizzato
- non comunicare via mail le credenziali amministrative
- identificare le persone autorizzate a richiedere l'aggiunta o la modifica di amministratori dei sistemi o delle applicazioni

Le password delle credenziali di accesso all'amministrazione dei sistemi:

- devono essere modificate, al momento dell'installazione di strumenti hardware o software, sostituendo quelle di default utilizzate dal produttore/installatore
- non devono essere conservate in chiaro, né trasmesse su canali non cifrati
- in caso di trattamento di dati sensibili e/o giudiziari o comunque di rilevanza strategica, devono essere "robuste" e non facilmente individuabili con attacchi di "forza bruta".

1.5. PROTEZIONE DEI DATI

1.5.1 BACKUP DEI DATI

L'amministratore di sistema è responsabile della corretta applicazione delle politiche di gestione dei backup e si attiene a quanto specificato nella *Procedura di backup, ripristino dei dati* adottata dall'organizzazione al fine di garantire la disponibilità dei dati.

L'amministratore di sistema inoltre deve:

- effettuare controlli periodici e test di ripristino per verificare l'efficacia delle procedure, l'integrità e la consistenza dei dati ripristinati.
- assicurarsi che le copie di backup siano 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. Se possibile le copie dei backup devono essere riposte in casseforti o armadietti ignifughi le cui chiavi sono conservate dl Titolare, da un Responsabile o personale identificato.
- richiedere alle società che svolgono servizi di backup in outsourcing l'attivazione del backup per i nuovi sistemi e applicazioni, la descrizione del sistema di funzionamento di backup, i LOG periodici di completamento delle operazioni di backup
- monitorare l'esito dei backup eseguiti ed in caso di anomalie darne pronta segnalazione al Titolare e/o Responsabile del Trattamento ed alle società di servizi informatici coinvolte
- mantenere aggiornato il sistema di backup, sia per quanto riguarda il software di base che il software applicativo, applicando le relative *patches* di aggiornamento e sicurezza

1.5.2 ANTIVIRUS E ANTIMALWARE

I sistemi antivirus devono essere mantenuti aggiornati ed efficienti. Gli aggiornamenti devono raggiungere tutte le postazioni ed i sistemi, inclusi i dispositivi portatili di ogni genere.

1.5.3 SISTEMI FIREWALL

I sistemi firewall devono:

- essere configurati alo fine di garantire adeguata protezione della rete contro i rischi di accesso non autorizzato.
- avere disabilitate le porte ed i servizi non necessari alle attività di servizio
- essere configurati con adeguati sistemi di allarme in caso di tentativi di accesso non autorizzato
- essere provvisti di LOG chiari e non alterabili che attestino le evidenze delle attività di rete

1.5.4 CIFRATURA O SEPARAZIONE DEI DATI

I dati sensibili e/o giudiziari contenuti in banche dati elettroniche devono essere trattati con tecniche di cifratura che li rendono intellegibili solo agli incaricati autorizzati, identificati mediante impiego di idonee credenziali di autorizzazione e solo in caso di necessità.

1.5.5 DISMISSIONE E RIUTILIZZO DEI SISTEMI E DEI SUPPORTI

Ogni qualvolta si dismette o si riutilizza un dispositivo elettronico o informatico che contiene dati personali è necessario adottare idonei accorgimenti e misure che garantiscano la cancellazione sicura o la distruzione dei dati. Prima di autorizzare il reimpiego dei supporto o dei sistemi prima di procedere allo smaltimento degli stessi, L'Amministratore di Sistema provvede alla cancellazione in sicurezza ogni informazione contenuta attraverso le procedure di

- *wiping* (sovrascrittura)

- formattazione *lowlevel* (basso livello)
- distruzione dei supporti mediante punzonatura, deformazione, disintegrazione fisica
- smagnetizzazione dei dispositivi di memoria basati su supporti magnetici

Se necessario avvalersi di soggetti terzi qualificati ed autorizzati che attestino l'esecuzione delle operazioni effettuate.

Le operazioni effettuate in caso di reimpiego o di smaltimento dei dispositivi e degli strumenti informatici debbono essere registrate, indicando il tipo di supporto riutilizzato o dismesso, il suo numero di inventario e la criticità dei dai contenuti

1.6 PROTEZIONE DEI SISTEMI

Nelle fasi di alla progettazione, implementazione ed installazione dei sistemi, deve essere effettuata un'analisi dei rischi per determinare le misure di sicurezza minime o idonee da adottare.

Tutti gli interventi tecnici che riguardano l'installazione, la modifica o l'eliminazione di uno dei dispositivi che interessano l'applicazione delle misure di sicurezza devono essere opportunamente documentati ed autorizzati ed essere accompagnati, se l'intervento è effettuato da terzi, dall'attestazione dell'installatore.

1.6.1 SISTEMI SERVER

Gli amministratori dei sistemi server (*System Administrator*) sono tenuti a rispettare le seguenti indicazioni:

- sistemi hardware, sistemi operativi, servizi ed applicazioni installati devono essere approvati dalla direzione
- le patches di sicurezza rilasciate dai produttori de devono essere installate nel minor tempo possibile
- il software utilizzato deve essere associato ad una licenza, in accordo alle specifiche del produttore
- i servizi non necessari devono essere rimossi/disabilitati, compatibilmente con le dipendenze del sistema in oggetto
- servizi, sistemi ed applicazioni non più supportati dai produttori devono essere rimossi
- i servizi di comunicazione telematica devono essere configurati, o sostituiti, con servizi con traffico in cifrato
- interconnessioni, connessioni remote e relazioni di fiducia tra sistemi possono essere configurate solo per specifiche e comprovate esigenze di servizio
- qualsiasi attività di amministrazione remota deve essere effettuata utilizzando canali sicuri (es. connessioni di rete con crittografia)

1.6.2 APPARATI DI RETE

Gli amministratori di rete (*Network Administrator*) nell'attività di configurazione e gestione degli apparati di rete sono tenuti a rispettare le seguenti indicazioni:

- le password di amministrazione dei router sono modificate, rispetto a quelle di default, e sostituite periodicamente
- le comunicazioni wireless devono essere cifrate, utilizzando i più recenti e sicuri sistemi di crittografia delle comunicazioni
- devono essere disabilitati i servizi che possono rappresentare un rischio per la sicurezza
- le modalità operative di installazione, configurazione ed aggiornamento, come pure gli schemi della rete debbono essere documentate ed aggiornate

1.6.3 DISPOSITIVI PORTATILI

I dispositivi portatili necessitano di un'attenzione maggiore nella protezione dei dati personali che contengono e nella tutela rispetto ai possibili tentativi di furto.
I dispositivi portatili devono:

- avere la password di accesso al BIOS (anche la medesima su tutti i dispositivi, per facilitare gli interventi di amministrazione). La password deve essere trascritta nel documento riservato contenente l'elenco delle password di amministrazione dei sistemi.

  L'avvio da supporto rimovibile deve essere disabilitato.
- se possibile abilitare la crittografia dei dati su hard disk
- l'assegnazione dei dispositivi portatili deve essere documentata, l'assegnatario riceve e firma il documento *Assegnazione dispositivi mobili* e ne rispetta le prescrizioni contenute

1.7 GESTIONE DEI LOG

L'amministratore di sistema effettua il costante monitoraggio dei sistemi al fine di prevenire e limitare gli effetti di eventuali incidenti di sicurezza. La registrazione e analisi dei LOG informatici rappresenta uno dei più efficaci strumenti di monitoraggio. I LOG devono riportare:

- autenticazione (*login*) e disconnessione (*logout*) degli Incaricati
- accesso ai dati
- modifica di funzioni amministrative
- connessioni di rete (in ingresso ed in uscita).

Ove possibile ogni voce di log deve contenere:

- data/ora dell'evento
- identificativo del dispositivo (indirizzo IP o altro)
- identità dell'utente
- identificativo del processo che ha generato l'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), gli access LOG Gli access LOG relativi agli accessi degli Amministratori di sistema, devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. Devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservati per un congruo periodo, non inferiore a 6 mesi.

1.8 GESTIONE DEGLI INCIDENTI DI SICUREZZA

Nella gestione degli incidenti di sicurezza gli amministratori di sistema devono:

- segnalare alla direzione ed ai Responsabili le criticità, le violazioni di sicurezza e gli eventi che indicano violazioni delle misure di sicurezza previste
- dopo una prima verifica dell'accaduto, riportare per iscritto i fatti, le evidenze oggettive e le valutazioni degli incidenti di sicurezza, identificando il livello di criticità dell'evento
- comunicare all'utenza tutte le attività tecnico sistemistiche che possano compromettere la continuità operativa dei sistemi informatici
- attenersi alla *Procedura di Disaster Recovery* adottata dall'organizzazione

1.9 CONTROLLI DI SICUREZZA

1.9.1 ANALISI DEI RISCHI

L'amministratore valuta i potenziali rischi di sicurezza derivanti dall'installazione, l'utilizzo e la gestione dei sistemi informatici ed elettronici, attraverso un'adeguata analisi dei rischi che tenga conto del valore delle risorse da proteggere, delle potenziali minacce di sicurezza, dei meccanismi di sicurezza.

1.9.2 AUDIT

L'Amministratore di Sistema conduce opportuni audit periodici di sicurezza sui sistemi informatici al fine di:

- identificare il livello di rischio cui le risorse sono esposte
- valutare l'efficacia e l'efficienza dei meccanismi di sicurezza utilizzati
- valutare le eventuali non conformità e le seguenti azioni correttive

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

1.10 DOCUMENTAZIONE TECNICA

Gli Amministratori di sistema provvedono alla documentazione e al tempestivo aggiornamento della stessa, in relazione a tutti i sistemi, banche dati, apparati di rete e sicurezza, applicazioni software nonché alle

procedure operative di installazione, configurazione ed aggiornamento delle strumentazioni informatiche e telematiche di competenza. Tale documentazione deve essere messa a disposizione alla direzione, agli amministratori di sistema ed ai soggetti incaricati per quanto di propria competenza.

Tutti i documenti riservati dei Sistemi Informativi obsoleti o non più necessari devono essere sminuzzati con apposito dispositivo distruggi-documenti prima di essere gettati nella spazzatura.