MOSTRA D'OLTREMARE

REGOLAMENTO AMMINISTRATORI DI SISTEMA

MOSTRA D'OLTREMARE

Premessa:

Il legislatore italiano ha promulgato negli ultimi anni una serie di norme riguardanti il tema della sicurezza delle informazioni.
Sono immediatamente individuabili due filoni principali, il primo a tutela ".. dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato.." ed il secondo a garanzia del buon funzionamento e protezione dei sistemi informatici (D.Lgs. 518/92 e Legge n.547/1993).
La normativa di riferimento per il primo filone è il Testo Unico sulla privacy, emanato con D.Lgs. 196/03, che abroga tutte le precedenti norme, come la Legge n. 675/1996 ed il D.P.R. n. 318/1999. Queste due ultime norme definivano una fantomatica figura di Amministratore delle password, che nulla aveva a che vedere con le mansioni di un attuale *Domain Administrator*: l'iter legislativo aveva stravolto l'idea iniziale di affidare solo ai sistemi informatici la conservazione delle credenziali di autenticazione, obbligando paradossalmente gli operatori coinvolti ad effettuare operazioni da considerare, nella migliore delle ipotesi, incidenti della sicurezza, o peggio, reati.
La confusione creata (a tutt'oggi vi sono organizzazioni che continuano ad avere figure preposte a gestire gli elenchi delle password degli utenti), non è stata risolta dall'introduzione del D.Lgs. 196/03. Con questa norma scompare la figura di amministratore delle password e si trasferiscono sul Titolare del trattamento (notoriamente vittima di analfabetismo informatico) le responsabilità organizzative e, meno opportunamente, anche le responsabilità tecniche.
Questa concentrazione formale di responsabilità sul Titolare del trattamento, non risolve in ogni caso il problema degli accessi, incontrollati ed incontrollabili, a tutti i dati personali e sensibili presenti nella rete aziendale, da parte degli Amministratori di Sistema.
Il Garante della Privacy ha emanato, nel provvedimento del 27 novembre 2008, una serie di prescrizioni volte a tutelare la riservatezza delle informazioni conservate nella rete aziendale, lasciando al singolo Titolare del trattamento la scelta delle modalità di applicazione più specifiche.
Successivamente il Regolamento UE 2016/679 e il D. lgs. 101/2018("decreto di armonizzazione del Codice Privacy al Regolamento UE") hanno agito sul livello di sicurezza dei dati ma non sulla definizione di Amministratore di sistema che resta definito cosi' come dal provvedimento 27 novembre 2008.
Il presente regolamento ha l'obiettivo di definire esattamente ruolo, compiti e responsabilità delle figure coinvolte in prima linea nella tutela della riservatezza, integrità e disponibilità delle informazioni.

MOSTRA D'OLTREMARE

Glossario:

- Account: insieme di funzionalità, strumenti e contenuti attribuiti ad un utente in un determinato contesto operativo. Attraverso l'account, il sistema informatico od anche il software applicativo, rende disponibili agli utenti contenuti e funzionalità personalizzati rispetto al proprio profilo di autorizzazione.
- Ads: Amministratore di Sistema (v. Artt. 1 e 12 del presente Regolamento)
- Agent: programma o componente software capace di risolvere delle problematiche interagendo con altri software.
- Audit: in ambito sicurezza informatica, è la valutazione tecnica manuale o sistematica misurabile di un sistema o di un'applicazione.
- Backdoor: (letteralmente porta sul retro) è un mezzo di accesso ad un sistema che aggira i meccanismi di sicurezza.
- Backup: (copia di sicurezza) operazione periodica di duplicazione su differenti supporti di memoria dei dati o dei programmi presenti sui dischi di personal computer o di server.
- Domain Administrator: (amm. di dominio) tipologia di amministratore di sistema con elevati livelli di autorizzazione (v. Allegato A). In caso di singolo dominio è equivalente all'Enterprise Administrator.
- Registro delle attività di trattamento: è un documento contenente una serie di informazioni riguardanti le attività del trattamento dei dati personali (art. 30 Regolamento EU /2016/679).
- Dump: modalità di backup dei database (DBMS) tramite la creazione di un file contenente dichiarazioni SQL per la definizione dello schema e per l'inserimento dei dati contenuti.
- Elenco Ads: documento obbligatorio previsto al punto 4.3 del Provvedimento del Garante della Privacy del 27 novembre 2008.
- Enterprise Administrator: Amministratore di Sistema al massimo livello di autorizzazione (v. Allegato A del presente Regolamento).
- Export: operazione di esportazione di dati o configurazioni da servizi o applicativi software.
- Log: (gergo nautico) pezzo di legno fissato ad una fune con nodi a distanza regolare lasciato galleggiare in mare, permette la misura approssimata della velocità della nave (da qui la misura convenzionale della velocità di una nave in nodi). (Informatica) registro cronologico degli eventi.
- Logbook: (gergo nautico) registro di navigazione dove annotare ad intervalli regolari velocità, meteo, forza del vento, oltre ad altri eventi significativi che si verificano durante la navigazione. (Informatica) documento di registrazione di tutti gli eventi (vedi Art. 11 del presente Regolamento).
- Log di accesso: (o Access Log) registrazione cronologica delle operazioni di accesso su singolo sistema / rete / dominio.
- Log di sistema: (o System Log) registrazione cronologica degli eventi significativi verificatisi in un singolo sistema.
- Profilo di autorizzazione: insieme di informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti.
- Registro degli incidenti alla sicurezza: registro dove annotare tutti gli eventi avversi con risvolti (o possibili risvolti) su riservatezza, integrità e disponibilità delle informazioni.
- Relazione attività Ads: misura prevista dall'art. 7 del presente Regolamento.
- Designato al trattamento: "Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità" (art. 2-quaterdecies d.lgs. 101/2018).

- Autorizzato al trattamento: “Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità” (art. 4-quaterdecies d.lgs. 101/2018).
- Responsabile del trattamento: con l’adozione del d.lgs 101/2018 la figura di Responsabile del trattamento, che prima poteva riferirsi a responsabile interno e/o esterno, resta ad esclusivo appannaggio del responsabile esterno.
- Roll-back: (lett. Rotolare indietro) annullamento delle ultime operazioni effettuate senza modifiche ai dati o alla configurazione.
- Share di rete: spazio di condivisione dei dati di rete.
- Snapshot: (lett. istantanea) salvataggio di una macchina (configurazione, applicativi e dati) ad un dato istante.
- System log: registrazione degli eventi di un singolo sistema.
- System state: salvataggio della configurazione di un sistema.
- Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali(art. 4 Regolamento EU 2016/679.
- Troubleshooting: (lett. eliminazione del problema) processo di ricerca logica e sistematica delle cause di un problema.

Art.1 – Definizione di Amministratore di sistema

1. In ambito informatico, l’Amministratore di Sistema è la figura professionale che si occupa della gestione e della manutenzione di un sistema di elaborazione e delle sue componenti.
2. Nell’ambito dell’organizzazione è possibile individuare tipologie specifiche di Amministratore di Sistema, differenziate per livello di autorizzazione e profilo (*Allegato A - Tipologia di Amministratore e profili di autorizzazione*).
3. Si possono individuare Amministratori di Sistema interni o esterni all’organizzazione, ai sensi dell’Art. 3 del presente Regolamento.

Art.2 – Requisiti di nomina

1. L'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Art.3 – Regole e modalità di nomina

1. Il Dirigente dei Sistemi Informativi, se designato dal Titolare come Designato al trattamento dei dati personali, nomina gli Amministratori di Sistema ai sensi dell'art. 2 del presente regolamento.
2. La nomina deve essere individuale, per iscritto e deve riportare:
    a. nome e cognome, codice fiscale, data e luogo di nascita, residenza dell'Amministratore di Sistema nominato;
    b. i riferimenti telefonici di reperibilità dell'Amministratore di Sistema nominato (per la sola gestione delle emergenze)
    c. le tipologie di Amministratore di Sistema ed il profilo di autorizzazione che si intende affidare alla persona fisica (domain, server, networking, backup, come riportato in Allegato A);
    d. le finalità dell'autorizzazione, con la specifica delle attività e dei compiti (gestione backup, gestione del dominio e degli account, ecc);
    e. l'ambito analitico di autorizzazione (fino a includere/escludere eventuali macchine o insiemi di macchine, dispositivi, servizi, applicativi).
3. L'Enterprise Administrator crea l'account personale dell'Amministratore di Sistema nominato ed associa il profilo minimo necessario secondo quanto stabilito dal Dirigente dei Sistemi Informativi. La password deve essere inserita nel sistema di gestione dell'autenticazione direttamente dalla persona fisica nominata o in alternativa, il sistema genera una password che comunica direttamente ed in modalità sicura sempre alla persona fisica nominata.
4. Il Dirigente dei Sistemi Informativi può affidare l'attività di Amministratore di Sistema a soggetti privati e pubblici esterni all'organizzazione, nominando direttamente o indirettamente gli Amministratori di Sistema Esterni. Ad essi si applicano tutti gli articoli del presente Regolamento.

Art.4 – Modalità di nomina indiretta

1. In caso di nomina indiretta è obbligatorio provvedere a quanto segue:
    a. il Dirigente dei Sistemi Informativi definisce in un documento le figure da nominare ed i relativi profili di autorizzazione;
    b. il Titolare del trattamento, su proposta del Dirigente dei Sistemi Informativi, provvede alla nomina del Titolare dell'azienda fornitrice quale Responsabile del Trattamento;

c. Il Responsabile nomina a sua volta gli Amministratori di Sistema secondo quanto previsto dal documento prodotto dal Dirigente dei Sistemi Informativi;
d. Il Responsabile invia:
    i. dichiarazione circa il possesso dei requisiti di cui all'Art. 2 da parte dei nominati
    ii. copia della nomina della persona fisica ad Amministratore di Sistema
    iii. dichiarazione circa la redazione ed aggiornamento del proprio registro dei trattamenti
    iv. dichiarazione sull'adempimento dell'obbligo di formazione degli Amministratori nominati, secondo quanto previsto dalla normativa privacy
e. il Dirigente dei Sistemi Informativi integra l'Elenco degli Amministratori di Sistema con l'inserimento dei nuovi amministratori nominati.

Art.5 – Formazione ed aggiornamento annuale

2. Al fine di migliorare il livello di sicurezza dell'organizzazione, il Dirigente dei Sistemi Informativi organizza con cadenza annuale, sessioni di formazione ed aggiornamento sui temi della sicurezza nel trattamento dei dati e su temi specifici connessi ai compiti di amministrazione di sistema

Art.6 – Aggiornamento registro dei trattamenti

1. Gli estremi identificativi delle persone fisiche nominate Amministratori di Sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati:
    a. in un "Elenco degli Amministratori di Sistema" conservato ed aggiornato a cura del Dirigente dei Sistemi Informativi;
    b. nel registro dei trattamenti.

Art.7 – Verifica delle attività e Relazione annuale

1. Il Direttore dei Sistemi Informativi verifica periodicamente, e con cadenza annuale, l'attività degli Amministratori di Sistema attraverso audit interni, al fine di accertarne la conformità alle mansioni attribuite e la rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti.
2. Il Direttore dei Sistemi Informativi redige annualmente la "Relazione sull'attività svolta dagli Amministratori di Sistema", i risultati degli audit interni, la conformità alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti, riportando in evidenza tutti gli interventi volti a migliorare il livello complessivo di sicurezza.
3. Il Direttore dei Sistemi Informativi si riserva di comunicare al Dirigente dei Sistemi Informativi e alla Direzione qualsiasi comportamento non conforme al presente Regolamento per gli opportuni provvedimenti del caso.

Art.8 – Registrazione degli accessi e degli eventi

1. I sistemi informatici ed i dispositivi di comunicazione devono integrare funzionalità di registrazione degli accessi e di altre tipologie di eventi, prevedendo la registrazione degli accessi logici (autenticazione informatica) da parte degli Amministratori di Sistema ai sistemi di elaborazione ed agli archivi elettronici.
2. Tutti gli eventi di tutti i sistemi e dispositivi infrastrutturali ritenuti vitali e critici (per sensibilità dei dati contenuti o in quanto connessi direttamente alla continuità di servizi) devono essere registrati.
3. Per un miglior controllo e governo dell'infrastruttura informatica dell'organizzazione, è opportuno estendere la registrazione a tutti gli eventi di tutti i dispositivi collegati.
4. Le registrazioni (access log e system log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità, adeguate al raggiungimento dello scopo di verifica per cui sono richieste.

Art.9 – Esportazione e conservazione dei log

1. 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 6 mesi. I log possono essere cancellati solamente alla scadenza dei 6 mesi.
2. La registrazione e l'esportazione dei log deve essere effettuata nei modi previsti nell' Allegato C - Modalità di registrazione, esportazione e conservazione dei log.
3. I supporti di memorizzazione contenenti i log sono conservati a cura del Dirigente dei Sistemi Informativi in un contenitore chiuso a chiave. L'accesso è precluso a tutto il personale interno ed esterno, inclusi gli Amministratori di Sistema.

Art. 10 – Sala macchine

1. La Sala Macchina è considerata "Zona di massima sicurezza"; solamente gli Amministratori di Sistema nominati hanno facoltà di accesso.
2. Deve essere mantenuta chiusa a chiave e protetta da adeguati sistemi di sicurezza fisica.
3. L'accesso al personale non autorizzato è vietato e devono essere apposti cartelli di avvertimento, come riportato in Allegato B – Cartellonistica.
4. Ogni singolo accesso del personale alla sala macchine deve essere registrato, ai sensi dell'Art. 11 del presente Regolamento. Eventuali tecnici esterni devono essere identificati, autorizzati e registrati.
5. L'eventuale accesso di personale esterno è autorizzato solamente sotto stretta sorveglianza di un Amministratore di Sistema nominato.

Art.11 – Libro di bordo Sala Macchine – Logbook

1. E' istituito il "Libro di bordo Sala Macchine" o "*Logbook* Sala Macchine" dove sono riportati tutti gli eventi sensibili alla riservatezza, integrità e disponibilità delle informazioni.
2. Nel "Logbook Sala Macchine" devono essere riportati tutti gli eventi, come:
    a. Registrazione accessi sala macchine di personale interno ed esterno
    b. Installazioni/Disinstallazioni/Modifica delle configurazioni hardware o software
    c. Lavori di riparazione e di manutenzione
    d. Riavvii attesi, crash inattesi, interruzioni di servizio o di alimentazione
    e. Problemi di impianti di comunicazione, alimentazione, protezione, antincendio e climatizzazione
    f. Attivazione degli allarmi (intrusione, temperatura, allagamento)
3. Ogni registrazione deve prevedere:
    a. Progressivo evento
    b. Data/Ora evento, inizio attività o ingresso
    c. Data/Ora chiusura evento, fine attività o uscita
    d. Sistemi e dispositivi coinvolti
    e. Tipologia intervento (software / hardware / networking)
    f. Operazione effettuata
    g. *Roll-back* possibile (si/no)
    h. Possibile impatto dell'evento/operazione (Basso / Medio / Alto)
    i. Eventuali problemi riscontrati
    j. Livello Emergenza (min = 0; MAX = 5)
    k. Eventuale azione correttiva, strategia di risoluzione Eventuale azione correttiva, strategia di risoluzione
    l. Tecnico/Responsabile di riferimento
    m. Operatori, tecnici intervenuti e Firma del compilatore
    n. Eventuali Note

Art.12 – Compiti e Responsabilità

1. I principali compiti di un Amministratore di Sistema sono i seguenti:
    a. Monitorare l'infrastruttura informatica di competenza attraverso l'analisi dei log, identificando e prevenendo potenziali problemi
    b. Introdurre ed integrare nuove tecnologie negli ambienti esistenti
    c. Installare e configurare nuovo hardware/software sia lato client sia lato server
    d. Applicare le patch e gli aggiornamenti necessari al software di base ed applicativo, modificare le configurazioni in base alle esigenze dell'organizzazione
    e. Gestire e tenere aggiornati gli account utente ed i relativi profili di autorizzazione
    f. Fornire risposte alle questioni tecniche sollevate dall'utenza, porre rimedio ai problemi/guasti tramite tecniche di troubleshooting

g. Pianificare e verificare la corretta esecuzione dei backup e delle repliche
h. Documentare le operazioni effettuate (*Logbook*), le configurazioni, le modalità di backup e di ripristino dei dati e dei sistemi, gli eventi e le soluzioni ai problemi
i. Ottenere le migliori prestazioni possibili con l'hardware a disposizione
j. Operare secondo le prescrizioni di sicurezza e le procedure interne previste

Art.13 – Revoca della nomina

1. Il Dirigente dei Sistemi Informativi può revocare l'incarico di Amministratore di Sistema in caso di:
    a. inadempienza o inosservanza delle prescrizioni di sicurezza
    b. violazione del presente Regolamento
    c. sopravvenuta mancanza dei requisiti ai sensi dell'Art. 2
    d. modifica del rapporto contrattuale di lavoro dell'Amministratore di Sistema
2. La revoca degli Amministratori di Sistema legati contrattualmente a fornitori esterni all'organizzazione è compito del Responsabile del trattamento, direttamente o su richiesta del Dirigente dei Sistemi Informativi provvede ad effettuare la comunicazione di revoca
3. In considerazione dei risvolti tecnici ma soprattutto di continuità ed affidabilità dei servizi, la revoca dell'incarico di un Amministratore di Sistema dovrà seguire la procedura indicata all'Art.14

Art.14 – Procedura di revoca degli Amministratori di Sistema

1. La revoca dell'incarico di un Amministratore di Sistema prevede le seguenti azioni da eseguire rigorosamente nell'ordine specificato:
    a. Verificare l'esistenza di eventuali servizi lanciati (erroneamente) con l'*account* dell'Amministratore di Sistema; assegnare al servizio un *account* specifico per l'esecuzione della tipologia di servizi interessata
    b. Controllare l'esistenza di eventuali *backdoor* (*account* o applicative, accessi remoti, autorizzate o non autorizzate) riferibili all'Amministratore di Sistema da disabilitare
    c. Nel caso non sia già esistente, creare un *account* amministrativo con lo stesso profilo di autorizzazione dell'Amministratore di Sistema da disabilitare, da assegnare al nuovo Amministratore di Sistema (sostituto)
    d. Disabilitare l'*account* dell'Amministratore di Sistema revocato
    e. Verificare che tutti i servizi collegati al profilo di autorizzazione dell'Amministratore di Sistema risultino perfettamente funzionanti
    f. Comunicare la disabilitazione dell'account di Amministratore di Sistema e la revoca dell'incarico alla persona fisica

Art.15 – Divieti e disposizioni

1. La Documentazione Interna dei Sistemi Informativi, in particolare la documentazione relativa all'infrastruttura di rete, alla configurazione dei sistemi o degli applicativi, alle impostazioni o abilitazioni degli utenti, deve essere conservata in luogo sicuro, preferibilmente non accessibile in rete. L'accesso a detta documentazione è consentito solamente al personale nominato Amministratore di Sistema, per il solo tempo necessario alla consultazione e all'aggiornamento.
2. E' vietato trasportare la Documentazione Interna dei Sistemi Informativi in qualsiasi formato o media all'esterno della sede dell'organizzazione. Il divieto include l'invio di mail/fax/lettere contenenti documentazione anche parziale, la compilazione o la risposta ad interviste/indagini di mercato effettuate tramite telefono/fax/lettera
3. Gli *account* e le relative password di livello Amministratore di Sistema non devono essere rivelate a nessuno per nessun motivo. E' vietato trasmettere in qualsiasi formato anche criptato dette informazioni
4. In caso di perdita di segretezza di una password di livello Amministratore di Sistema, è necessario comunicare l'evento al Dirigente dei Sistemi Informativi, annotarlo nel Registro degli incidenti alla sicurezza, effettuarne immediatamente la modifica e verificare che non siano stati creati nel frattempo nuovi utenti o modificati profili di autorizzazione
5. Qualora giungano richieste telefoniche da parte dell'Autorità Giudiziaria o degli organi di polizia è necessario richiedere l'identità del chiamante; si provvederà a richiamare non direttamente l'interno, avendo così la certezza sull'identità del richiedente (call-back)
6. In Allegato D sono riportate le "Linee guida e note operative" specifiche per gli Amministratori di Sistema.

MOSTRA D'OLTREMARE

Allegato A - Tipologia di Amministratore e profili di autorizzazione

1. Sono state individuate le seguenti tipologie ed il relativo profilo di autorizzazione

Tipologia	Livello Sicurezza	Ruolo	Profilo di autorizzazione
Enterprise Administrator 	MAX	Livello più alto di autorizzazione nell'ambito della rete dell'organizzazione. Nel caso di singolo dominio le figure di Enterprise Administrator e Domain Administrator coincidono.	Autorizzato: 1. all'accesso completo a tutti i dati e a tutte le macchine appartenenti a tutti i domini della rete (a meno di diversa ed esplicita configurazione); 2. alla creazione degli *account* ed abilitazione degli accessi agli Administrator di livello 0, 1 e 2 di tutti i domini; 3. all'analisi e controllo dei log di tutte le macchine appartenenti a tutti i domini e dei dispositivi di tutta la rete.
Domain Administrator 	0	Livello più alto di autorizzazione nell'ambito del singolo Dominio della rete dell'organizzazione. Nel caso di singolo dominio le figure di Enterprise Administrator e Domain Administrator coincidono.	Autorizzato: 1. all'accesso completo a tutti i dati ed a tutte le macchine appartenenti ad un singolo dominio della rete (a meno di diversa ed esplicita configurazione); 2. alla creazione degli *account* e all'abilitazione degli accessi agli Administrator di livello 0, 1 e 2 del solo dominio di appartenenza; 3. all'analisi e controllo dei log di tutte le macchine appartenenti al solo dominio di appartenenza e dei dispositivi della porzione di rete gestita.
Server Administrator 	1	Amministratore di un singolo sistema server.	Autorizzato: 1. all'accesso completo al sistema ed ai dati contenuti nel server (a meno di diversa ed esplicita configurazione; es. escluso db); 2. a compiere qualsiasi operazione sistemistica e di modifica della configurazione del server; 3. all'analisi e controllo dei log.

MOSTRA D'OLTREMARE

Account Administrator 	1	Amministratore degli *account* utente per il solo dominio di appartenenza.	Autorizzato: 1. alla creazione/disabilitazione degli *account utente*; 2. all'assegnazione del profilo di autorizzazione all'*account utente*.
Network Administrator 	1	Amministratore dell'infrastruttura di rete e di comunicazione	Autorizzato: 1. all'accesso completo ai dispositivi di comunicazione (es. router, switch, hub, centrale telefonica) ed alle linee di comunicazione; 2. a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di comunicazione; 3. all'analisi e controllo dei log, del traffico dati e telefonico.
Security Administrator 	1	Amministratore dei dispositivi di sicurezza	Autorizzato: 1. all'accesso completo ai dispositivi di sicurezza (es. Firewall, Antivirus, Log Management, Traffic analyzer); 2. a compiere qualsiasi operazione di modifica della configurazione dei dispositivi di sicurezza; 3. all'analisi e controllo dei log.
Data Base Administrator 	1	Amministratore di un database server o di una singola istanza di database	Autorizzato: 1. all'accesso completo al motore del database ed ai dati memorizzati; in casi particolari è possibile autorizzare anche la singola istanza di database; 2. a compiere qualsiasi operazione di modifica della configurazione e degli schemi dei database; 3. all'analisi e controllo dei log.
Backup Administrator 	1	Amministratore dei backup e delle repliche dei dati	Autorizzato all'accesso (almeno in lettura): 1. dei dump dei database (o direttamente delle istanze in caso di utilizzo di *agent*); 2. delle *share* di rete; 3. dei *system state* e degli *snapshot* delle macchine;

			4. delle configurazioni (che necessitano di backup); 5. degli *export* di specifici servizi; 6. dei log di tutte le macchine della rete.
Service / Application Administrator 	2	Amministratore di un singolo servizio o applicazione (es. mail server, web server, application server)	Autorizzato: 1. alla gestione, modifica delle configurazione, stop/start del singolo servizio o applicazione; 2. all'analisi e controllo dei log specifici del servizio o applicazione.
Local Administrator - Technical support 	2	Amministratore locale di singoli sistemi *client*	Autorizzato: 1. all'accesso completo ad un insieme specificato nella nomina di sistemi *client* ed ai dati contenuti nei dispositivi di memorizzazione (a meno di diversa ed esplicita configurazione); 2. all'analisi e controllo dei log locali.

Allegato B – Cartellonistica

MOSTRA D'OLTREMARE

Allegato C – Modalità di registrazione, esportazione e conservazione dei log

1. I sistemi informatici ed i dispositivi di comunicazione devono prevedere spazi adeguati di memorizzazione dei log; la capacità deve essere almeno doppia rispetto al massimo riscontrato tra una esportazione e la successiva.
2. Caratteristiche di mantenimento dell'integrità dei dati raccolti dai sistemi di log sono in genere disponibili nei più diffusi sistemi operativi, o possono esservi agevolmente integrate con apposito software o con strumenti di esportazione e salvataggio.
3. E' necessario effettuare l'esportazione periodica dei dati di log su supporti di memorizzazione non riscrivibili, con riportato periodo, data di salvataggio, tipologia di log su file LEGGIMI.TXT ed anche direttamente sul supporto con pennarello indelebile.

4. Il supporto deve essere controfirmato dal Dirigente dei Sistemi Informativi con pennarello indelebile o con firma digitale della cartella contenente i log (anche in formato compresso).
5. Nel caso fosse disponibile il servizio di certificazione della data, è consigliata l'apposizione di un Timestamp digitale direttamente alla cartella compressa dei log.
6. Non è esclusa la possibilità di implementazione di sistemi più sofisticati, come log server centralizzati, sempre che sia possibile certificare e firmare digitalmente i log.

Allegato D – Linee guida e note operative

1. Attenersi scrupolosamente a tutte le procedure operative e segnalare immediatamente al Dirigente dei Sistemi Informativi qualsiasi evento o situazione, anche solamente sospetta, che possa compromettere il buon funzionamento del Sistema Informativo.
2. Tenere meticolosamente aggiornata la documentazione dell'infrastruttura di rete, dei sistemi e delle configurazioni, come anche l'inventario hardware e software.
3. Effettuare con la massima diligenza tutti i controlli inclusi nelle TO DO LIST e CHECK LIST previste nelle procedure operative.
4. Pianificare e comunicare preventivamente all'utenza tutte le attività tecnico sistemistiche che possano compromettere la continuità operativa dei sistemi informatici.
5. Tutti i documenti dei Sistemi Informativi devono essere sminuzzati con apposito dispositivo prima di essere gettati nella spazzatura.
6. Tutti i media o dispositivi di memorizzazione (cd, dvd, hard disk, nastri, penne usb, ecc.) devono essere formattati a basso livello, riscritti a livello di traccia o completamente distrutti prima di essere conferiti in discarica.
7. In caso di invio di un media in assistenza tecnica o in riparazione, assicurarsi che sia realmente illeggibile.
8. Ad ogni logon amministrativo deve corrispondere un logout anche nel caso di assenza temporanea; ad ulteriore sicurezza deve essere impostato lo screen saver protetto con password, con tempo di attivazione inferiori ai 5 minuti.
9. Utilizzare sempre il livello di utente minimo necessario ad effettuare il compito amministrativo richiesto (non usare Administrator/root/Qsecofr se non necessario)

10. Cambiare le password relative ad account amministrativi di livello 2 ogni 3 mesi e le password amministrative di livello più alto almeno ogni mese; per il lancio di servizi o di specifici compiti utilizzare solamente utenze dedicate, con possibilità di modifica della password ad intervalli semestrali.
11. Al personale di supporto esterno, anche se nominato Amministratore di Sistema, è vietato il collegamento alla rete o direttamente ai dispositivi dell'Azienda, di qualsiasi strumento non di proprietà dell'organizzazione (ad esempio notebook, penne usb, ecc.).
12. Il personale esterno deve produrre documentazione preventiva in relazione ai lavori ed alle modalità che intende seguire per svolgere il compito assegnato; al completamento del lavoro deve essere consegnata:
    a. la Dichiarazione di Conformità che attesti la rispondenza alle disposizioni del Disciplinare Tecnico Allegato B - Decreto Legislativo n. 196/2003 ed alle altre norme vigenti (tutela del software, ecc.);
    b. la documentazione minuziosa sul lavoro svolto e le eventuali note o differenze rispetto al progetto;
13. La sala macchine deve essere mantenuta pulita, ordinata, sgombra da qualsiasi oggetto o involucro non direttamente connesso con alla rete dell'organizzazione.
14. E' tassativamente vietato fumare, bere o portare quanto non strettamente necessario in sala macchine; sostare per il solo tempo necessario ad effettuare il compito assegnato.