

Rinnovo Documento Programmatico per la Sicurezza (DPS) Scadenza 31 Marzo 2010

Gentile Cliente,

il 31 marzo scade il termine annuale per il rinnovo del Documento Programmatico per la Sicurezza (DPS) in relazione al trattamento dei dati elettronici in azienda.

Il documento quest'anno **dovrà riportare le attività messe in atto** relativamente alle novità introdotte sull'obbligo di adozione delle procedure in materia di spazzatura elettronica, posta elettronica e soprattutto a seguito dell'obbligo inerente **l'amministratore di sistema entrato in vigore il 15 dicembre scorso** (provvedimento che peraltro obbliga all'adozione di informative, nomine e formalizzazioni specifiche per taluni fornitori esterni).

Secondo le **norme** fissate dal Garante Privacy, tutti i titolari che dispongono di un sistema informatico devono indicare nel DPS i riferimenti dell'**amministratore di sistema**, prevedendo **verifiche di conformità annuali**, anche in relazione alle modalità di autenticazione e accesso logico ai sistemi di elaborazione e memorizzazione.

Alleghiamo, a scopo riassuntivo della norma, il comunicato relativo alla **descrizione degli adempimenti della normativa inerente gli Amministratori di Sistema** e, di seguito, **la proposta di Macro Group inerente la gestione e il controllo degli "Access log"** che consente alle Aziende di assolvere alle specifiche richieste del Garante in modo semplice ed efficace.

Restando a Vostra disposizione per ogni chiarimento in merito e per un' eventuale formulazione di offerta inerente la Vostra struttura, previo inoltrare della **richiesta di quotazione del servizio**, compilata in ogni sua parte, Porgiamo i nostri migliori saluti.

Macro Group Spa

Studio Legale Avvocato Valentina Frediani
Foro di Pistoia

www.consulentelegaleinformatico.it
www.consulentelegaleprivacy.it

Oggetto: Descrizione adempimenti della normativa inerente gli Amministratori di Sistema

Scade il 15 dicembre prossimo, l'obbligo di adozione del provvedimento normativo in materia di amministratore di sistema.

Il provvedimento si applica alle grandi imprese (**tutte, a prescindere dai dati trattati**) ed alle piccole e medie imprese che, oltre ai dati contabili - amm.vi e dati sensibili dei dipendenti, trattano dati che rientrano nelle tipologie di seguito riportate:

- Dati dei potenziali clienti (in quanto non raccolti in adempimenti di un accordo contrattuale, ma antecedentemente per attività di natura promozionale);
- Dati giudiziari (si pensi a dati relativi a contenziosi, recupero crediti o dati inerenti a fornitori);
- Dati relativi ai dipendenti in materia di connessione ad internet od in adempimento di qualificazione del personale presso il fornitore;
- Dati raccolti mediante sistemi di videosorveglianza;
- Dati raccolti mediante siti web (newsletter);
- Dati di natura sensibile per quanto concerne titolari di trattamenti specifici;
- Dati di rilevazione geografica;

e via dicendo.

Di conseguenza, il provvedimento obbliga il titolare o il responsabile a verificare ed individuare nominativamente gli amministratori di sistema, che dovranno poi essere muniti di profili di autorizzazione univoci per accedere ai sistemi ed operare.

Sotto il profilo prettamente documentale, ciascun titolare del trattamento dovrà individuare gli amministratori di sistema interni ed esterni, redigere apposite nomine, realizzare documento descrittivo del recepimento della normativa contenente tutti i riferimenti in merito agli ADS nominati, integrare l'informativa ai dipendenti ed assumere idonee garanzie circa il trattamento dei dati gestiti da terzi anche in forma di outsourcing.

Dal punto di vista tecnico-informatico del provvedimento, occorrerà predisporre (**obbligatoriamente ed in tutti in casi**) sistemi di registrazione degli accessi logici (autenticazione per l'accesso) ai sistemi di elaborazione ed agli archivi elettronici; le registrazioni dovranno comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate, conservando gli **access log** registrati per minimo 6 mesi (conservazione in modo completo ed inalterabile dei log) con obbligo di verifica annuale dell'operato degli amministratori di sistema da parte del titolare o del responsabile.

L'omissione dell'adozione di queste misure di sicurezza potrà generare responsabilità sia penali (art. 169 decreto legislativo n. 196/2003) che sanzionatorie (ad esempio in caso di omissione di informativa, art 161 decreto legislativo n. 196/2003).

Avv. Valentina Frediani
via Cividale n.51 - 51016 Montecatini Terme (PT)
Tel. +39-0572-78166 Fax +39-0572-72698
vfrediani@consulentelegaleinformatico.it
Skype: consulentelegaleinformatico.it

LA SOLUZIONE MACRO GROUP PER IL CONTROLLO DEGLI ACCESS LOG

“Misure e accorgimenti prescritti ai titolari dei trattamenti dati effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema (Riferimento al documento del Garante per la Privacy G.U. n. 300 del 20 dicembre 2008)”.

Dal 15 dicembre prossimo decorre l'obbligo di adozione del provvedimento normativo in materia di amministratore di sistema che il Garante della Privacy ha emesso. Un provvedimento che richiede l'implementazione da parte di tutte le organizzazioni sia pubbliche che private, di un processo di controllo degli accessi logici ai sistemi informatici da parte degli amministratori.

Il decreto, richiede che:

“Vengano 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.”

Una forte enfasi è posta quindi sulla necessità per l'Azienda di verifica dell'attività svolta dall'amministratore di sistema ed è quindi necessario da un punto di vista informatico:

- **Dotarsi** di un sistema di controllo che consenta di registrare gli accessi effettuati dagli amministratori di sistema;
- **Registrare** ogni operazione in appositi audit log:
 - Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo non inferiore a 6 mesi;
 - Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità;
- Far sì che l'operato degli amministratori di sistema sia oggetto di un'**attività di verifica**, con cadenza almeno **annuale**, da parte dei titolari del trattamento per controllarne la sua conformità rispetto alle misure di sicurezza;
- **Introdurre** per tutti i Titolari dei trattamenti le misure in oggetto entro il **15 dicembre 2009**.

Inoltre, da un punto di vista documentale, ciascun titolare del trattamento dei dati dovrà:

- a) individuare gli amministratori di sistema interni
- b) individuare gli amministratori di sistema esterni
- c) redigere appositi documenti in relazione alle mansioni svolte (leggi incarichi)
- d) integrare il documento programmatico di sicurezza
- e) integrare l'informativa ai dipendenti
- f) assumere delle garanzie contrattualistiche circa il trattamento dei dati gestiti da terzi anche in forma di outsourcing.

Quali le conseguenze giuridiche del mancato adempimento?

“L’omissione dell’adozione di questa misure di sicurezza potrà generare responsabilità anche di tipo penale oltre che a conseguenze eventualmente sanzionatorie in caso di omissione o mancata integrazione di taluni documenti previsti nel provvedimento (sanzioni amministrative sino a 120.000 euro)”.

La normativa completa relativa alla "registrazione degli accessi" e' visibile sul relativo sito del Garante: <http://www.garanteprivacy.it/garante/doc.jsp?ID=1580831>

Macro Group propone un servizio di **gestione e controllo degli “access log”** che consente alle Aziende di assolvere **alle specifiche richieste del Garante** in modo semplice ed efficace.

Il servizio proposto

Il servizio viene erogato da Macro Group in modalità Outsourcing (il motore di elaborazione dati, installato presso il nostro data center, raccoglie con un protocollo criptato via internet i dati inviati da un collettore software installato sul server del Cliente che si occuperà di raccogliere i log dai vari sistemi).

Centralmente il personale tecnico di Macro Group si assume il compito di:

- Verificare e segnalare eventuali anomalie di comunicazione tra il collettore (installato presso il Cliente) ed il server (installato negli uffici Macro Group);
- Memorizzare tutti i log su supporto ottico adeguato da inviare al Cliente con cadenza predefinita e concordata;
- Inviare al Cliente report periodici;
- Dare disponibilità al Cliente di crearsi report di controllo in tempo reale consentendo l’accesso via internet.

Perchè adottare la nostra soluzione?

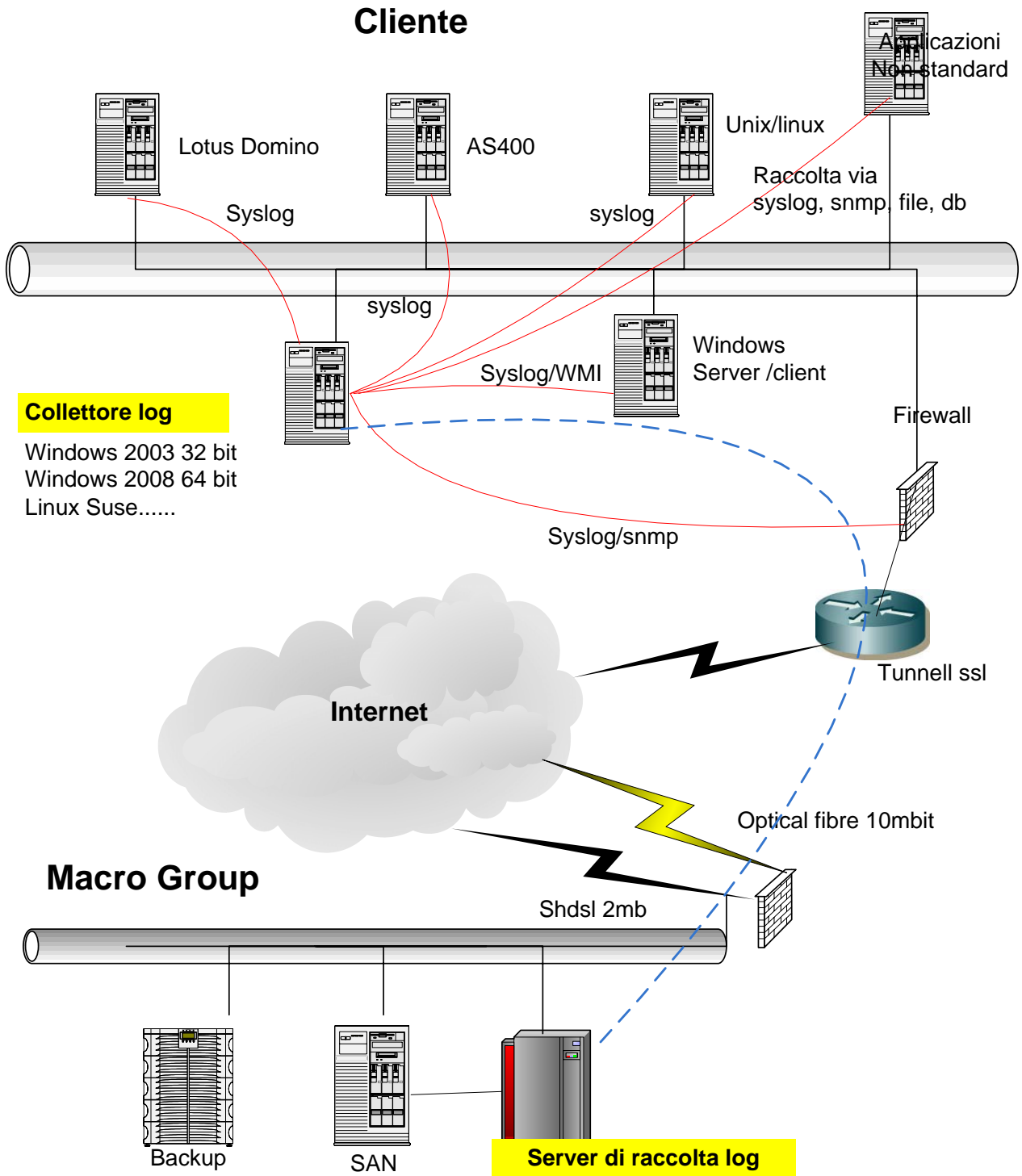
- Riduce i costi iniziali che derivano dall'applicazione della normativa;
- Abbatte i costi a regime;
- Garantisce un’elevata qualità ed efficienza del servizio;
- E’ la base per avere un utile servizio di Network Monitoring a basso costo (controllo delle attività critiche della infrastruttura tecnologica quali salvataggi non andati a buon fine, rottura e malfunzionamento degli apparati e dei sistemi, ecc.).

Il servizio può essere attivato in qualsiasi architettura di rete esistente senza la necessità di apportare variazioni significative.

Moltissimi sono i dispositivi supportati, a partire dai più diffusi sistemi operativi, Windows, Linux, OS400, apparati firewall, antivirus, etc.

E' una modalità operativa assolutamente non invasiva che può essere implementata e resa operativa in brevissimo tempo a costi particolarmente contenuti.

Revisione:	0.1
Data:	24/10/2009
Documento:	Privacy
Pagina:	1 / 1



FLUSSI OPERATIVI - SPECIFICHE TECNICHE

Il Cliente:

1. deve individuare le unità da monitorare (as400, server, firewall ecc.)
2. deve individuare la macchina su cui installare il Collettore dei log (pc o server, Windows o linux *) la cui installazione ordinariamente viene effettuata in modalità remota, così come le eventuali e successive manutenzioni. Tale attività, su esplicita richiesta del Cliente, può essere effettuata presso la sede del Cliente con separato addebito
3. Implementare ed aggiornare la tabella degli "Amministratori di Sistema"

Il Fornitore:

1. deve istruire i vari sistemi e/o apparati dell'esistenza del collettore in grado di ricevere informazioni di log, ovvero :
 - 1.1. su AS/400 viene installato un programma che raccoglie i log e li spedisce al collettore via syslog
 - 1.2. su Windows vengono attivati i servizi WMS/WMI, in alternativa si configurerà un syslog o altri metodi (*)
 - 1.3. su Lotus Domino viene installato un DB che filtra i log degli amministratori e poi vengono spediti al collettore via syslog
 - 1.4. su Unix/linux viene configurato syslog o snmp
 - 1.5. sugli apparati di rete viene attivato syslog o snmp

* Se debbono essere monitorate macchine windows VMI/WMS, il collettore dovrà essere installato su una cpu windows 2003 32 bit oppure Windows 2008 64 bit.

Il Software:

Premesso che il software è in grado di raccogliere qualsiasi tipo di dato o messaggio, sia che venga generato da "applicazione specifica" o dai sistemi operativi delle unità sottoposte a rilevazione.

Il software è in grado di interpretare i messaggi provenienti dagli apparati e dalle applicazioni standard: ciascun messaggio di log proprietario si può configurare, rilevare e rendere leggibile.

Una volta parametrizzato ciascun dispositivo, al software:

- vengono indicate le tipologie dei messaggi che devono essere inoltrati al collettore (filtro)
- ovvero, vengono trascurati tutti i messaggi non di interesse all'applicazione.

Il collettore: Installato su un elaboratore già disponibile presso il Cliente

- raccoglie tutti i messaggi provenienti dai singoli apparati,
- li firma elettronicamente (il dato grezzo, generato dal sistema o applicazione, viene firmato – hash -)
- li protocolla per garantire la “non modificabilità” e la sequenza di arrivo, per eliminare la possibilità che vengano cancellati alcuni log.
- Ciascun log ricevuto, avendo esso forma e contenuto eterogeneo, viene normalizzato (viene affiancato al dato originale un dato leggibile e/o interpretabile e visualizzabile).
- in funzione della frequenza di inoltro dei dati concordata tra il Cliente e Macro Group (secondi, minuti, ore, giorni)
 - Si connette al server di Macro Group , creando un tunnel vpn
 - trasmette i dati in maniera protetta
 - a conferma del ricevimento avvenuto, vengono rimossi dal sistema che li ha inoltrati.
- Segnala al “Server di raccolta LOG” l’eventuale interruzione di comunicazione con una delle unità da cui deve rilevare i dati

Il Server di raccolta LOG, residente presso il data center Macro Group:

- comunica al collettore mittente l’avvenuta ricezione dei dati,
- cripta i dati ricevuti,
- salva giornalmente i dati,
- produce periodicamente dei report (sintetici ed analitici) che saranno inoltrati al Cliente con periodicità da concordare
- su esplicita richiesta del Cliente, potranno essere concordate altre forme di consultazione e/o inoltro dei dati,
- i dati vengono conservati, in più versioni, per un periodo di 6/12 mesi
- Segnala al Cliente l’eventuale interruzione di comunicazione con il Collettore

**INFORMATIVA POTENZIALI CLIENTI IN MATERIA DI PROTEZIONE DEI DATI PERSONALI AI SENSI
DELL'ART. 13 D. LGS. 30.06.2003, N. 196**

In osservanza di quanto previsto ai sensi e per gli effetti dell'art. 13 D. Lgs 30 giugno 2003, la **MACRO GROUP S.p.A.** con sede in BOLOGNA, 40068 San Lazzaro di Savena, via Emilia 292, nella sua qualità di titolare del trattamento dati, in persona del legale rappresentante pro-tempore, informa i potenziali clienti sulle finalità e modalità del trattamento dei dati personali raccolti, il loro ambito di comunicazione e diffusione, oltre alla natura del loro conferimento. E nello specifico informa su:

FINALITA'

I dati raccolti presso i potenziali clienti, oggetto del trattamento, sono trattati ed utilizzati direttamente per adempiere a finalità strumentali al compimento dell'attività informativa tenuto conto delle attività da Voi svolte.

I dati sono stati raccolti a seguito di contatto telefonico con la struttura di appartenenza o in occasione di manifestazioni/fiere/incontri di tipo commerciale e/o attingendo da DB acquisiti dal titolare del trattamento.

I dati saranno trattati in conformità ai principi di correttezza e liceità come anche alle disposizioni di legge.

MODALITA'

Il trattamento dei dati è eseguito attraverso procedure informatiche o comunque mezzi telematici o supporti cartacei ad opera di soggetti interni appositamente incaricati. I dati sono conservati in archivi cartacei, informatici e telematici e sono assicurate le misure di sicurezza minime previste dal legislatore.

COMUNICAZIONE E DIFFUSIONE

I dati personali non saranno diffusi, venduti o scambiati con soggetti terzi.

I DIRITTI DI CUI ALL'ART. 7

L'interessato potrà far valere i propri diritti come espressi dall'art. 7, 8, 9 e 10 del D.Lgs. 30 giugno 2003 n. 196, rivolgendosi al titolare del trattamento. In particolare secondo l'art. 7 l'interessato potrà ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile. L'interessato ha diritto di ottenere l'indicazione: a) dell'origine dei dati personali; b) delle finalità e modalità del trattamento; c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2; e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati. L'interessato ha diritto di ottenere: a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati; b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati; c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato. L'interessato ha diritto di opporsi, in tutto o in parte: a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta; b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

TITOLARE

Titolare del trattamento è la **MACRO GROUP S.p.A.** con sede in BOLOGNA, 40068 San Lazzaro di Savena, via Emilia 292,. I diritti di cui alla presente informativa sono esercitabili inviando apposita istanza al suddetto indirizzo.

TEMPI DI CONSERVAZIONE

I dati saranno conservati per un periodo non superiore a quello necessario per gli scopi per cui sono stati raccolti o successivamente trattati e comunque l'interessato potrà esercitare il diritto di cancellazione in qualsiasi momento.

Richiesta Quotazione Servizio di raccolta e gestione access log Amministratori di Sistema

per ottemperare alla normativa inerente "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" (G.U. n. 300 del 20 dicembre 2008).

Tipologia di servizio richiesto	
Indicare il n° di dispositivi interessati dal processo	
X	Attivazione del servizio - "una tantum"
	Fino a 5 dispositivi*
	Fino a 10 dispositivi*
	Fino a 15 dispositivi*
	Oltre 15 dispositivi*

**Per dispositivi si intende ogni apparecchiatura informatica in grado di gestire accessi o contenere dati strutturati.*

SOCIETA'	_____
INDIRIZZO	_____
LOCALITA'	_____
TELEFONO	_____
E-MAIL	_____
REFERENTE	_____

Inoltare il modulo di richiesta quotazione all'indirizzo marketing@macrogroup.it
o via fax al n° **0516229798**

Mittente

Spett/le
Macro Group S.p.A.
Via Emilia, 292
40068 San Lazzaro di Savena (BO)

**ORDINE PER L'ATTIVAZIONE DEL SERVIZIO
di raccolta e gestione access log Amministratori di Sistema**

per ottemperare alla normativa inerente "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" (G.U. n. 300 del 20 dicembre 2008).

Fascia	Tipologia di servizio richiesto
	Attivazione del servizio fascia A/B c/o Macro Group
A	Fino a 5 dispositivi
B	Fino a 10 dispositivi
	Attivazione del servizio fascia C c/o Macro Group
C	Fino a 15 dispositivi
D	Oltre 15 dispositivi

Indicare il tipo di fascia prescelto (A/B/C/D): _____

Prezzo concordato: _____

Periodo del servizio: Per il primo anno si intende dal 15 dicembre 2009 al 31 dicembre 2010.
Successivamente dal 1 gennaio 2011 si intende l'anno solare.

Modalità di fatturazione: Annuale, anticipata

Pagamento richiesto: RB 30gg d.f.f.m.

N.B.

- Per dispositivi si intende ogni apparecchiatura informatica in grado di gestire accessi o contenere dati strutturati.
- Al seguente ordine seguirà contratto di servizio di outsourcing.
- Eventuali attività svolte presso la sede del Cliente saranno addebitate alle tariffe in essere.

Data, _____

Timbro e Firma

ALCUNE REFERENZE
ACCESS LOG

