



Empower your Business with Our Solutions
ERP • CRM, IP Contact Center Solutions • Telemarketing Software

SISECO INFORMA "PRIVACY"

Copie di Sicurezza (Backup)

E

Gestione Password

10 Agosto 2007

PREMESSA

Gentile Cliente, vorremmo sottoporre alla tua attenzione un breve promemoria su alcuni aspetti della **gestione dati** che potrebbe risultare di importanza vitale per la tua Azienda; *chiediamo solo pochi minuti del tuo prezioso tempo !*

Ricordiamo che la legge sulla **PRIVACY** prevede:

Art. 31 (Obblighi di sicurezza)

*"I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da **ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi**, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta."*

Questo significa avere un adeguato sistema di **BACKUP** che permetta di eseguire giornalmente le copie dei dati, così da essere salvaguardati in caso di danni o catastrofi naturali.

Ricordiamo inoltre che **GAT.Crm**[®] è già **PRIVACY-READY**

Tutti i requisiti di sicurezza richiesti dall'allegato tecnico "B" della legge sono presenti ed ampiamente configurabili (es. durata, complessità, lunghezza minima delle password, compatibilità con Active Directory di Microsoft, ...)

Alcune note generali sull'aggiornamento di GAT.Crm

- Effettuare di preferenza gli **aggiornamenti** quando vengono pubblicati, oppure almeno ogni due/tre rilasci. Questo consente di avere **GAT** sempre aggiornato, senza cambiamenti troppo "traumatici" tra una versione e l'altra.
Nota: l'assistenza viene erogata per l'ultima versione rilasciata e le precedenti tre versioni. Le versioni più vecchie non vengono più supportate.
- Prendere nota di quale sia la postazione **PRIMARIA** e farla sempre partire per prima ad inizio di ogni mese. Se ci sono più database, ricordarsi di accedere ad ognuno per attivarli correttamente.
- Effettuare gli aggiornamenti sempre cominciando dalla postazione **PRIMARIA**.
- Se le postazioni sono molte, è possibile creare una funzione automatica che **aggiorna tutte le postazioni** client.
- Leggere sempre ed a fondo le **Note di Rilascio**: ogni versione è corredata da questo importante documento che illustra l'operatività della nuove funzioni.
- Se possibile, attivare **l'assistenza remota**: in caso di problemi i controlli saranno **più veloci ed efficaci**. Non è necessario lasciare sempre attiva l'assistenza remota, questa può essere attivata "on demand" e/o solo in caso di problemi (es. accendere i servizi VNC solo quando necessario e spegnerli subito dopo aver terminato l'assistenza, oppure cambiare di frequente le password).

COPIE DI SICUREZZA e BACKUP: alcuni consigli pratici

Copie di sicurezza ed aggiornamenti... un vantaggio anche per te!

BACKUP E CONSERVAZIONE DELLE COPIE



- Controllate ogni giorno che vengano eseguite le **copie di sicurezza**, e che successivamente siano copiate su supporti **esterni** al server e conservate **lontano** dal server stesso (in un'altra stanza, oppure presso il titolare/responsabile)
- Le copie dovrebbero essere fatte preferibilmente in modo **giornaliero** e dopo il termine del lavoro. In caso di ripristino si avranno così dati sempre recenti.
- Se si cambia il server o si crea un nuovo database, controllare che le **schedulazioni** dei backup siano impostate correttamente. Se avete impostato le **copie automatiche da GAT**, controllare che il servizio "Agent" di SQL sia avviato: infatti se quest'ultimo risultasse "spento", le copie schedulate non verranno eseguite.

Nota per chi ha installato SQL 2005 EXPRESS:

In SQL2005 EXPRESS il servizio "Agent" è stato rimosso. Per poter continuare ad avere le copie di sicurezza "in automatico" è possibile:

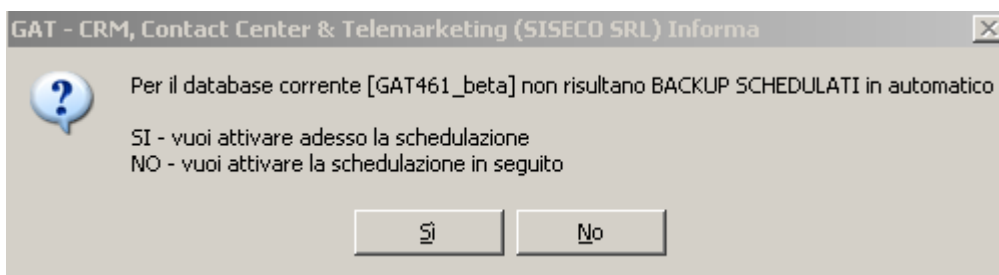
- passare a SQL2005 WORKGROUP o STD
- impostare un sistema di backup esterno a GAT

FUNZIONALITA' IN GAT.crm

In GAT, nelle "Opzioni" dell'utente (Utilità / Opzioni, nella linguetta "Generali") è presente questa funzionalità:

Avvisa controllo Backup Automatici <input checked="" type="checkbox"/>	Avvisa quando dimensione archivio supera i	1.800	MB - 0 non avvisa
	Avvisa quando LOG supera il numero di righe	1.000.000	NR - 0 non avvisa

Avvisa controllo backup automatici: se GAT rileva che non sono stati impostati dei backup nell'apposita pagina di Gestione Database Server, avvisa l'utente ad ogni accesso con un messaggio simile al seguente:



Premendo **SI**, viene aperta la maschera di Gestione Database Server, dove è possibile schedulare l'evento, indicando la frequenza (settimanale, giornaliera, mensile, ecc), la cartella dove deve essere salvato il file e l'orario.

Premendo **NO**, si può proseguire a lavorare con GAT, ma questo non imposta un backup.

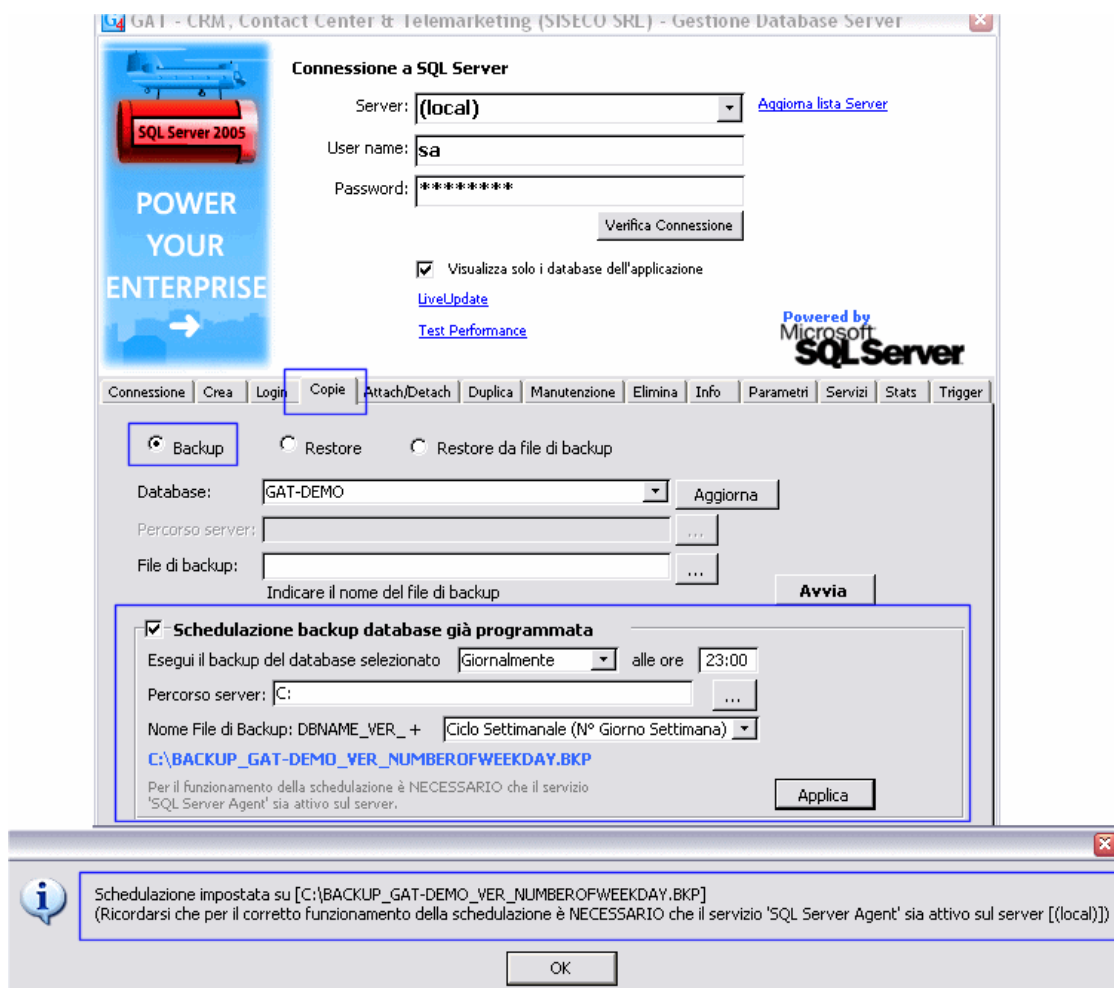
SCHEDULAZIONE AUTOMATICA IN GAT.crm

All'interno della Gestione Database Server nella pagina "COPIE" è possibile attivare la schedulazione automatica del Backup di un database.

Il sistema verifica automaticamente che in base alla versione di SQL Server presente sia possibile usufruire del sistema SQL Agent per la schedulazione automatica.

E' possibile definire diverse opzioni:

- frequenza del backup (giornaliera / settimanale)
- posizione del backup
- semantica del nome del backup, al fine di stabilire un ciclo di backup
 - o infinito
 - o settimanale
 - o mensile
 - o annuale



Ricordiamo inoltre di provare periodicamente anche la funzionalità dei backup, simulando un "restore" (ripristino della copia dei dati dal supporto sul pc). Questo è da eseguirsi preferibilmente su un pc staccato dalla rete e che non contenga dati per evitare di sovrascrivere i dati odierni con quelli del backup.

Accesso sicuro alle informazioni (Cambio periodico delle PASSWORD)

La password protegge la tua Privacy, previene intrusioni e mette al sicuro i dati !

Il costante controllo di questo aspetto è previsto dalla legge sulla **Privacy** che – come sicuramente ben saprete - impone la normativa per la sicurezza dei dati. Ricordiamo che per essere conformi, le password devono contenere:

- almeno una lettera maiuscola
- almeno una lettera minuscola
- almeno un numero
- almeno un carattere speciale (# @ ? ! + [] * / \ | % & \$ £ ecc)



La password "standard" di GAT è **12345Aa!**

Vediamo alcuni aspetti che si possono collegare facilmente all'uso quotidiano e pratico di GAT e del PC.

Ricordate sempre che la password ha un ruolo importante per la sicurezza dei dati e dell'azienda!

Cosa si trova in Gestione Utenti

In Gestione Utenti è possibile visualizzare quando è stata fatta l'**ultima modifica della password (1)**, dell'**ultimo accesso in GAT (2)**, la **scadenza della password (3)** ed il **ruolo dell'utente nel "trattamento dei dati" (4)**.

IDUtente	Nome Utente	Utente Windows	Ruolo Utente	Ultimo Accesso
ADMIN	ADMIN	TITOLARE DEL TRATTAMENTO	0,00	06/08/2007 - 12.45
	Amministratore <input checked="" type="checkbox"/>	N° funzioni disponibili	222	Gestione
	Utente avanz.* <input checked="" type="checkbox"/>	Password (1 car.min.)	*****	Tutte
	Disabilitato ** <input type="checkbox"/>			Cambia
	Utente Visibile in Login <input checked="" type="checkbox"/>			Nessuna
Data/ora inserimento	Data/ora ult.modifica	Utente ult.modifica	Numero modifiche	
01/01/2005	19/07/2007 12.10.49	DEBUG	762	
Ultimo Cambio Pwd	10/02/2006 - 15.45			

Indicare che un utente è un operatore di telemarketing dell'archivio. Ad esempio un operatore può vedere solo i suoi contratti. Queste modifiche richiedono di ripetere il processo.

COSA PUO' FARE UN UTENTE AVANZATO

Cambio della password in GAT

La modifica può essere fatta a cura dell'amministratore oppure dell'utente stesso. In caso di modifica da parte dell'**amministratore** è sufficiente entrare in GESTIONE UTENTI, posizionarsi sulla scheda dell'utente interessato e cliccare sul pulsante "**cambia**" (5)

Non è necessario che l'amministratore conosca la vecchia password dell'utente, in quanto viene riproposta in automatico da GAT (non è comunque visibile a video).

NOTA: l'amministratore ha la facoltà di cambiare le password di tutti gli utenti, mentre i singoli utenti possono modificare solo la propria.

In caso di modifica da parte dell'**utente** stesso, è sufficiente cliccare col tasto destro del mouse sull'icona di GAT che compare vicino all'orologio del pc e selezionare la voce "Cambio Password", dopodichè digitare la nuova password.

Se l'utente non dispone dell'icona di GAT sopra indicata, può premere la combinazione di tasti "**CTRL + F3**" da qualsiasi punto del programma.

Infine, sulla maschera principale di GAT viene indicato quanti giorni mancano al cambio della password:




Oltre alle password di accesso in GAT esiste anche la password di sicurezza per il collegamento a **SQL**, che consigliamo vivamente di non lasciare **mai vuota**.

Di norma quando viene installato il motore **MSDE** sul server la password **non viene definita**. Può comunque essere **inserita velocemente** in seguito utilizzando le funzioni presenti in Utilità / Gestione Database Server nella linguetta "LOGIN".

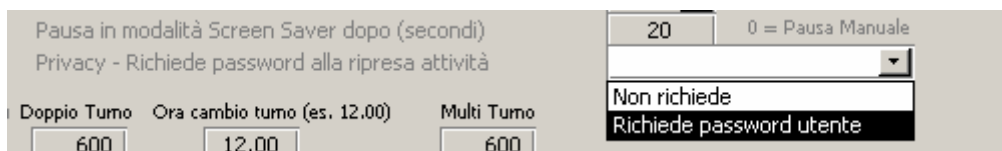
Pause e Screen Saver

Dalla versione GAT 461, nelle "Opzioni" dell'utente (Utilità / Opzioni, sulla linguetta "Registro In/Out") sono state inserite due nuove funzioni:

- **Pausa in modalità Screen Saver dopo (secondi)**: questa funzione si attiva quando

l'operatore preme il tasto . Se è impostata a "zero", l'operatore dovrà premere manualmente il tasto per segnalare la pausa; se invece viene inserito un valore, GAT va automaticamente in pausa dopo N secondi di inattività.

- **Privacy: richiede password alla ripresa attività: le opzioni disponibili sono:**
 - non richiede: quando l'operatore torna dalla pausa riprende semplicemente l'attività senza dover inserire la password
 - richiede password utente: quando l'operatore torna dalla pausa deve inserire la propria password per poter riprendere l'attività



Parametri della procedura

Nel menu Utilità, alla voce "Parametri della Procedura", abbiamo a disposizione dei parametri specifici per la gestione e la modifica "obbligatoria" delle password.

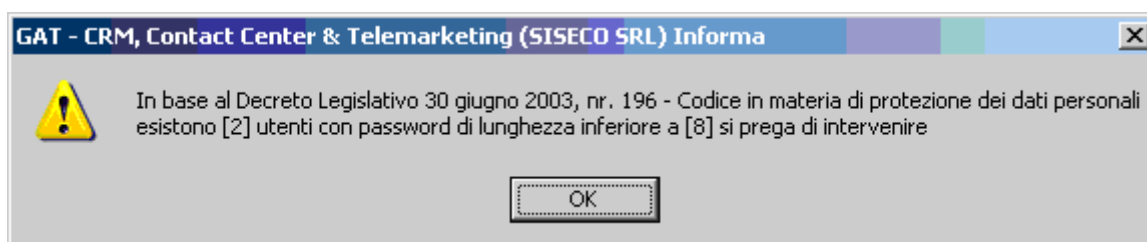
Parametro	Descrizione	Valore Default	Valore Consigliato
ELU004	Privacy: numero minimo caratteri password	8	8
ELU005	Privacy: abilita conformità Password ai requisiti di complessità (a-z,A-Z,0-9,!£\$%...)	SI	SI
ELU006	Privacy: disabilita utente a seguito di N tentativi di accesso errati (0=Nessun limite)	0	3
ELU008	Privacy: disabilita utente dopo N giorni di mancato utilizzo (0=Nessun limite)	0	30
ELU009	Privacy: impedisce utilizzo delle ultime N password (0=Nessun limite)	0	3
ELU013	Privacy: richiedi cambio password obbligatorio dopo N giorni (0=Nessun limite)	0	90

Per attenersi alle disposizioni, consigliamo vivamente di impostare a **SI** il parametro **ELU005** (abilita la conformità della password ai requisiti di legge).

Inoltre è previsto che la password debba essere **modificata periodicamente**, cosa che può essere effettuata tramite l'impostazione del parametro **ELU013**.

Ricordiamo infine che i parametri possono essere personalizzati a livello utente.

Se GAT dovesse rilevare che alcuni utenti posseggono una password non conforme, avviserà l'amministratore con un messaggio simile al seguente:



I sistemi operativi Windows98, Windows98SE ed inferiori non possiedono i requisiti di sicurezza previsti dalla legge.

Ricordiamo che dall'11 luglio 2006 Microsoft non rilascerà più alcun supporto tecnico per i sistemi **Windows 98, Windows 98 SE e Windows Millennium Edition (Me)**.

Da questa data in poi, infatti, non verranno più rilasciate patch di aggiornamento per i sistemi sopra citati, il che espone i PC obsoleti ad elevati rischi in termini di sicurezza.

Come creare password efficaci

Come già accennato, la **password** è il più importante **strumento che permette di salvaguardare i dati riservati** dagli sguardi indiscreti o da "letture accidentali" da parte di persone che non devono venire a conoscenza di dati riguardanti l'azienda.

Purtroppo non sempre si dà il giusto peso all'**efficacia** della propria password, a volte per mancanza di tempo oppure per non dover ricordare password complesse ed astruse.

Innanzitutto è utile porsi i seguenti quesiti:

- Usate password che altri potrebbero indovinare facilmente, come il nome della moglie / marito / figli, oppure il modello di auto?
- Utilizzate parole di senso compiuto?
- Scegliete di memorizzare la password in modo da non doverla digitare ogni volta?
- Annotate le password su post-it che poi incollate al monitor, oppure sull'ultima pagina dell'agenda sempre presente sulla scrivania?
- L'azienda ha una password che è uguale per ogni pc?
- La password è sempre la stessa da molti anni?

Se la risposta è sempre SI, allora i dati presenti nei vostri computer sono esposti ad eventuali "attacchi" e l'applicazione delle password **non è ottimale**.

Ecco i rischi che comportano password non complesse, accompagnati da alcuni suggerimenti utili:

Password facili da indovinare: se al vostro computer hanno accesso anche altri colleghi, è probabile che questi siano a conoscenza di informazioni private come il vostro secondo nome, oppure quello dei familiari. **Il primo consiglio** quindi è: evitate di utilizzare i nomi, soprannomi, il proprio indirizzo, il nome dell'animale domestico, la marca dell'auto, la targa, la propria data di nascita, di matrimonio, il luogo dell'ultima vacanza, il telefilm/film preferito, ecc. Più in generale quindi, **evitate di utilizzare informazioni note o facilmente reperibili**.

Parole di senso compiuto: evitate di utilizzare parole facili per le password, è più sicuro utilizzare una combinazione di lettere, numeri e simboli: esistono programmi che consentono di identificare le password basate su parole di senso compiuto in più lingue.

Password automatiche: quando leggete la posta direttamente dal sito, scrivete la password ogni volta, cercando di evitare la funzionalità che permette la memorizzazione dei dati. Come per le parole di senso compiuto, sono disponibili programmi poco costosi o persino gratuiti che consentono anche la decodifica degli asterischi usati per mascherare le password.

Annotazione delle password: le password sono utili solo se le si ricorda, ma annotarle in post-it o sull'agenda e lasciarlo alla portata di tutti non è una soluzione opportuna. Se si dispone di più password, puoi archivarle in un file, proteggendole a loro volta con una password realmente efficace e che siete in grado di ricordare.

Utilizzo della stessa password: molti utenti usano la stessa password per qualsiasi pc o collaboratore. Questo evita di tenere a mente un gran numero di password differenti, ma implica il rischio che altri possano accedere a qualsiasi dato presente. Ancora una volta vale la regola di usare password differenti, ma soprattutto di **modificarle spesso**.

Password complesse

Una password complessa ha le seguenti caratteristiche:

- E' composta di almeno otto caratteri, e in ogni caso più lunga è meglio è
- Include maiuscole, minuscole, numeri e simboli speciali

- Viene cambiata di frequente
- la nuova password è sempre sensibilmente differente dalla precedente

Alcuni esempi di password complesse:

- **[P&CO]!a><321**
- ***Z@a00(b(aA7?**

Queste password sono difficili da decifrare. Purtroppo sono anche difficili da ricordare, soprattutto se sono numerose e tutte con questo livello di complessità.

Quasi tutti i sistemi operativi di ultima generazione (**escluso Windows 98**) supportano le password complesse, ma soprattutto ci permettono di creare password sotto forma di frase, che risultano così più facili da ricordare. Ad esempio:

- (!Si ke vinciamo con 100 punti!)
- [10 minuti di BICI son tanti?]

Un sistema valido per costruire una password complessa consiste nello scrivere una frase facilmente memorizzabile utilizzando solo la prima lettera di ogni parola. Per esempio:

- | | | |
|---|---------|------------|
| • L'Inquilino del 5 piano è Insopportabile! | diventa | LId5*pèI! |
| • A Natale mi compro due paia di sci | diventa | ANmic2pdS |
| • Oggi lavoro dalle 9 alle 15 | diventa | Old9alle15 |

Possiamo inoltre unire diverse parole tramite numeri e simboli. Per esempio:

- Meridiano0[Greenwich]-1h
- Maratona_è_42Km+195m
- Natale+Ferie: 23Dic/07Gen

Ci sono quindi svariati modi per creare password facili da ricordare: una volta capito il meccanismo diventa relativamente facile anche modificarle periodicamente.

Una volta create password complesse o in forma di frase, ci sono ancora alcuni punti da tenere in considerazione per garantire la riservatezza:

- Sconnettersi sempre dal sistema quando si deve lasciare il PC incustodito, oppure mettere uno screen-saver che entra in funzione dopo un minuto e protetto da password
- Cambiare le password almeno ogni 90 giorni
- Non condividere le password con nessuno

Sfruttando l'efficacia delle password complesse, potrete finalmente garantire alle informazioni riservate la segretezza che meritano.

**Per cambiare la password del pc è sufficiente premere
CTRL + ALT + CANC e scegliere la voce "cambia password"**