b.com by GAT.core

BusinessCOntactManagement

PRIVACY & SECURITY

Gestione Password e Backup

Validità: Giugno 2019

SOMMARIO

1. Introduzione

BCOM è una piattaforma sviluppata e realizzata da impresoft srl per i clienti che hanno come core business attività Commerciali, vendita e gestione ed assistenza Clienti.
La piattaforma, modulare, web, innovativa e altamente personalizzabile consente di automatizzare rapidamente i processi di Sales, Marketing e Post-Sales.

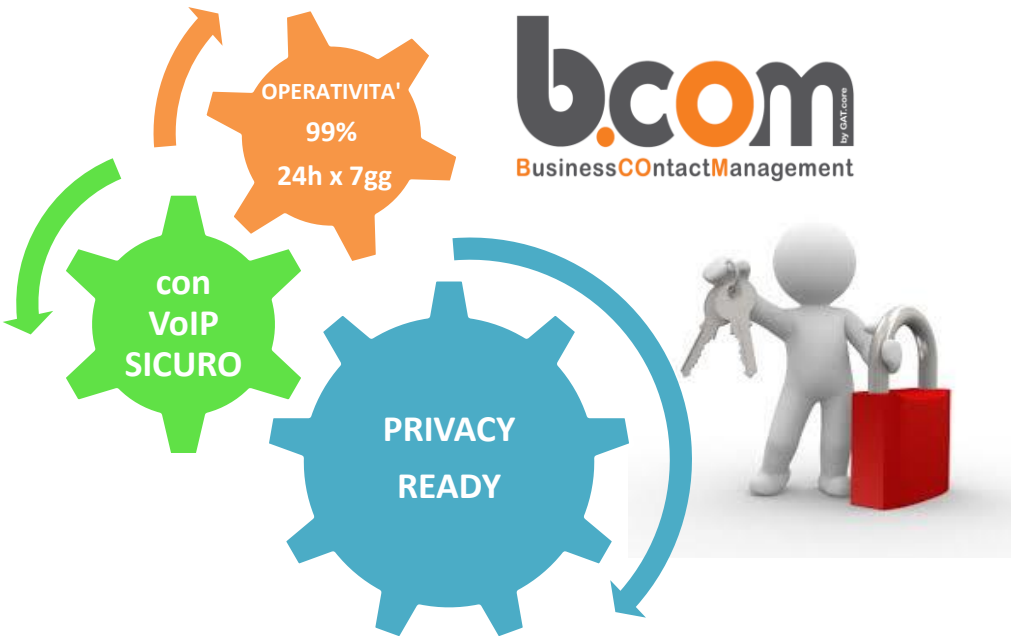
impresoft srl, è certificata ISO 9001, nell'ambito delle procedure di progettazione, sviluppo, installazione, integrazione ed assistenza di piattaforme software evolute per la gestione di CRM, Multimedia Contact Center e sistemi CTI.
Per garantire la selezione di controlli di sicurezza adeguati e proporzionati, adotta lo standard ISO 27001 relativamente al ISMS (Sistema di Gestione della Sicurezza delle Informazioni.

La piattaforma BCOM ®by impresoft è installabile e fruibile in modalità:

- **ON DEMAND** (modalità Saas con noleggio a canone flat e/o utente/mese)
- **CLOUD COMPUTING** (es: Nuvola Italia di Telecom Italia)
- **ON PREMISE** (Licenza installata presso il cliente)

La piattaforma è integrabile con centralini IPHONE BOX – VOIP, per la gestione delle chiamate entranti e uscenti, e col modulo Predictive per la gestione automatica delle chiamate uscenti.

A seconda della tipologia di installazione sono espletate direttamente da impresoft alcune attività di gestione, manutenzione, sicurezza, back up, assistenza.



2. Gestione Backup e Privacy

La normativa

Nell'utilizzo del CRM occorre porre attenzione su alcuni aspetti sulla **riservatezza** nella **gestione dati** che potrebbero risultare di importanza vitale per l'Azienda.

Ricordiamo che la legge sulla **PRIVACY (DL N°196 del 30 giugno 2003 e successivi aggiornamenti)** all'**art. 31** (Obblighi di sicurezza) prevede quanto segue.
"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 evitare l'accesso non autorizzato o un trattamento non consentito o non conforme alle finalità della raccolta**."

Questo significa avere un sistema CRM con:

- **Un adeguato sistema di BACKUP** che permetta di eseguire giornalmente le copie dei dati, cosi da essere salvaguardati in caso di danni o catastrofi naturali.
- **Una gestione dell'accesso e uso delle informazioni sicuro e tracciabile**

Il **CRM è già PRIVACY-READY,** infatti tutti i requisiti di sicurezza richiesti dall'allegato tecnico "B" della legge sono presenti ed ampiamente configurabili nel CRM (es. durata, complessità, lunghezza minima delle password, compatibilità con Active Directory di Microsoft, ...).

La Responsabilità

In virtù della normativa è utile ricordare che la RESPONSABILITA' ultima per il corretto utilizzo dei sistemi informatici e in modo particolare ai punti sopra esposti, ricade in capo al RAPPRESENTANTE LEGALE della società.

Aggiornamento del CRM

La prima regola per avere un CRM sempre sicuro e allineato alle ultime novità funzionali, è quella di effettuare, di preferenza, gli **aggiornamenti** quando vengono pubblicati, oppure almeno ogni due/tre rilasci.
Questo consente di avere **il CRM** sempre aggiornato, senza cambiamenti troppo "traumatici" tra una versione e l'altra. Leggere sempre ed a fondo le **Note di Rilascio**: ogni versione è corredata da questo importante documento che illustra l'operatività della nuove funzioni.
L'Assistenza impresoft è disponibile per fornire il supporto in caso di problemi o di chiarimenti. Si tenga presente che l'assistenza viene erogata per l'ultima versione rilasciata e per le tre versioni precedenti.
Le versioni più vecchie non sono supportate.

Backup dei dati del CRM

Regole di Backup

Alcuni semplici regole da applicare regolarmente:

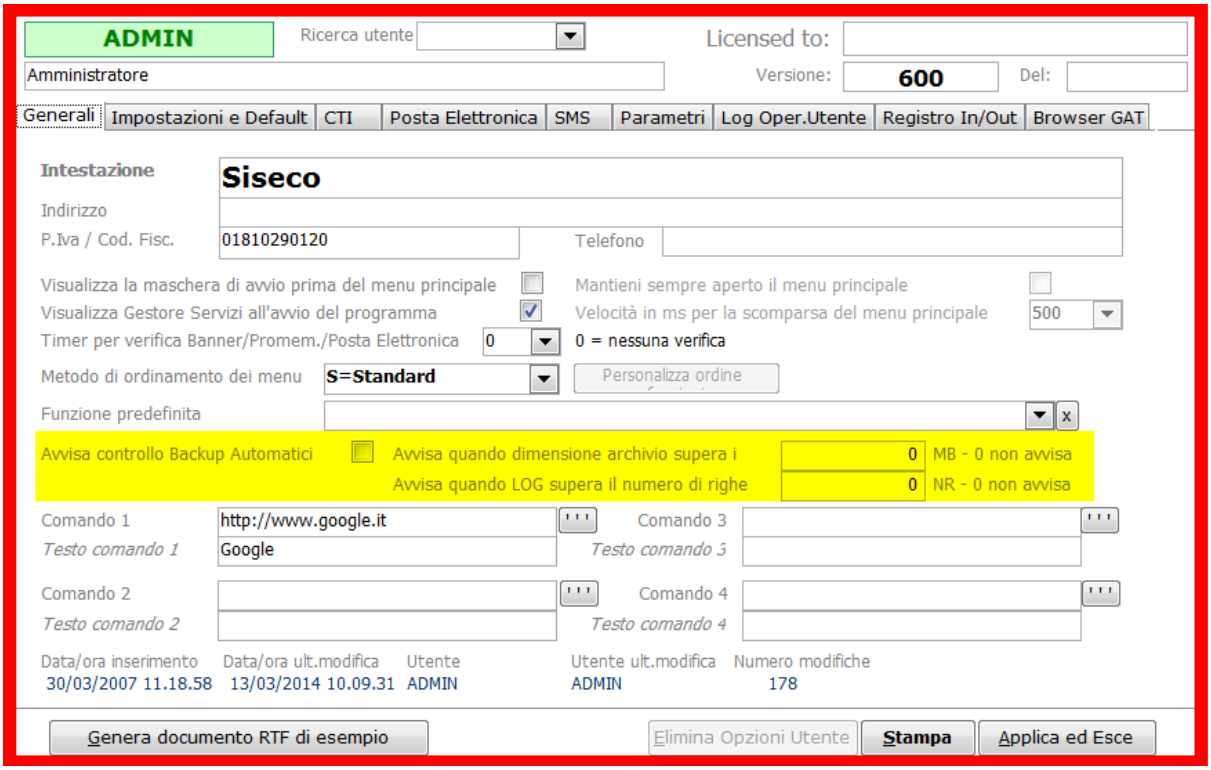
- Controllate ogni giorno che vengano eseguite le i **Backup** (**copie di sicurezza)**, e che successivamente siano copiate su supporti **esterni** al server e conservate **lontano** dal server stesso (in un'altra stanza, oppure presso il titolare/responsabile).
- Le copie dovrebbero essere fatte preferibilmente 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 CRM/CS**, 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 in versione EXPRESS si consideri che il servizio "Agent" non è presente. Per poter continuare ad avere le copie di sicurezza "in automatico" è possibile:

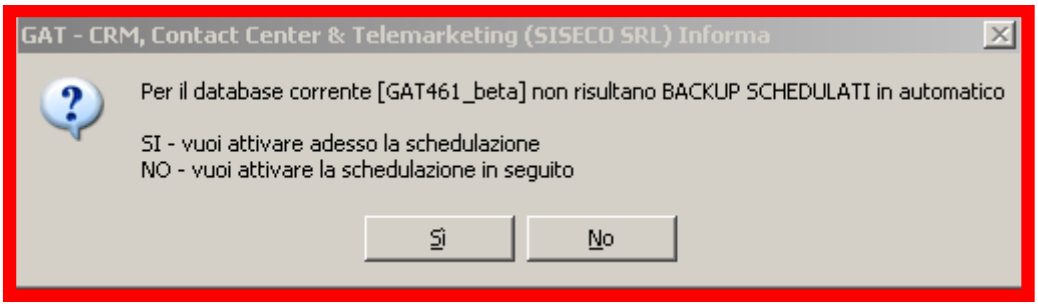
- passare a SQL in versione WORKGROUP o STD
- impostare un sistema di backup esterno al CRM

Configurazione del Backup con CRM/CS

In CRM/CS, in Utilità / Opzioni, nel tab "Generali" è presente la funzionalità **Avvisa controllo backup automatici** (in giallo):



Se CRM/CS 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:



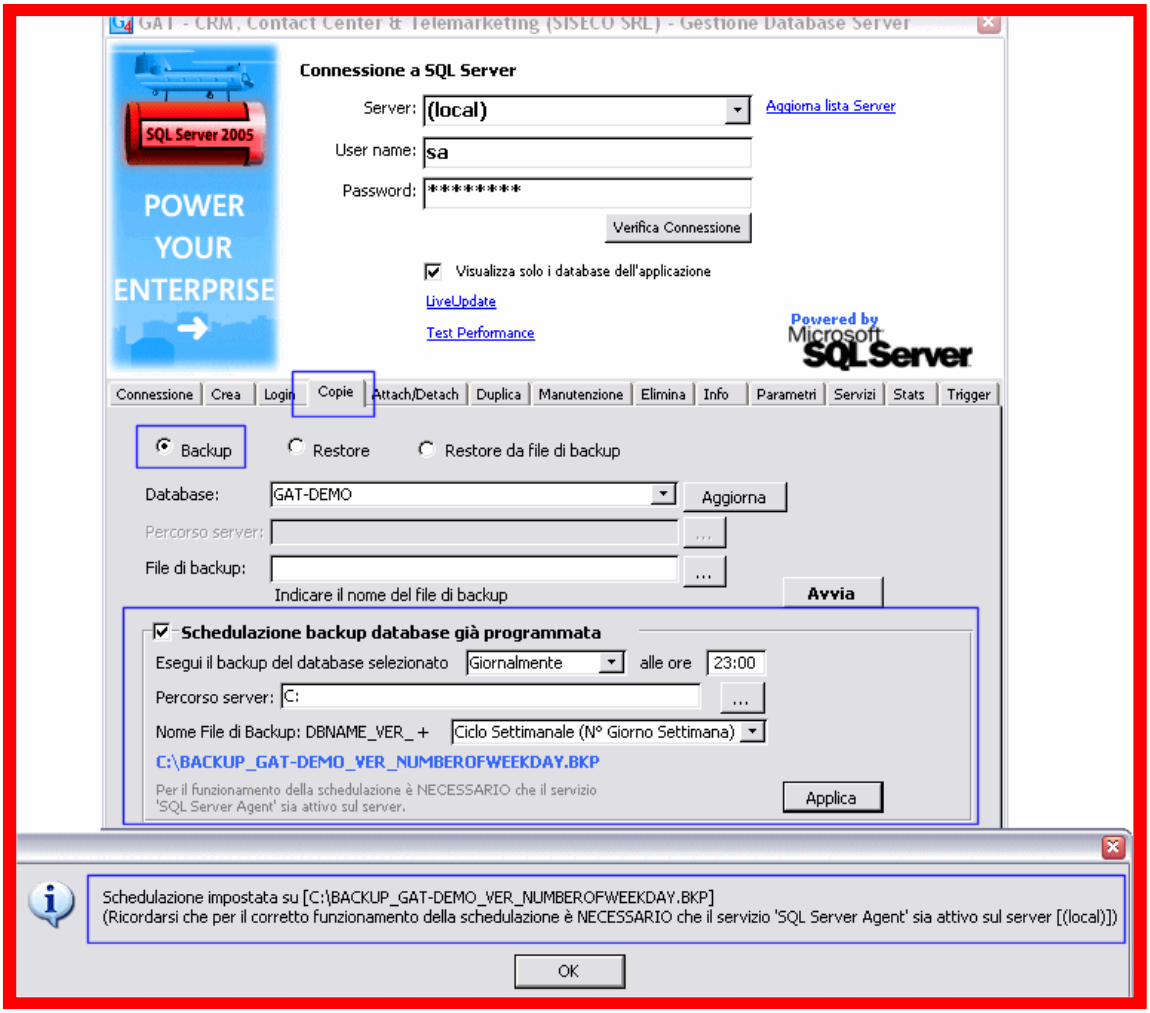
Premendo **SI**, viene aperta la maschera di Gestione Database Server, dove è possibile schedulare l'evento, indicando la frequenza (settimanale, giornaliera, mensile, ecc), la cartella dove deve essere salvato il file e l'orario.
Premendo **NO**, si può proseguire a lavorare con CRM/CS, ma questo non imposta un backup.

Schedulazione automatica tramite CRM/CS

In CRM/CS, in Utilità / Gestione Database Server, nel tab “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
  - infinito
  - settimanale
  - mensile
  - annuale



Ricordiamo inoltre di provare periodicamente anche la funzionalità dei backup, attuando un ripristino DB su una nuova connessione del CRM.

HTTPS - L'accesso sicuro al CRM

Accesso

L'accesso alla piattaforma avviene a mezzo di una connessione Internet a banda larga a cura dell'utente, mediante l'utilizzo di uno dei seguenti browser e con utilizzo del protocollo HTTPS.

Tipo di Browser Client	FIREFOX (3.x.x)	GOOGLE CHROME	IE8/IE9 * (32/64BIT)	IE10/IE11 * Desktop (32/64BIT)	SAFARI
BCOM	✓	✓	✓	✓	✓
Piattaforma CLIENT	**Win**	**Win**	**Win**	**Win**	**Win**

✓ = certificato
✓ = utilizzabile con alcune funzionalità ridotte dovute al browser
* = la "modalità compatibilità" deve essere disabilitata

L'URL di collegamento alla piattaforma si basa su un protocollo di crittografia HTTPS [HyperText Transfer Protocol over Secure Socket Layer], tale protocollo viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti che potrebbero essere effettuati tramite la tecnica di attacco del "man in the middle".

In pratica viene creato un canale di comunicazione criptato tra il client e il server attraverso uno scambio di certificati. Questo tipo di comunicazione garantisce che solamente il client e il server siano in grado di conoscere il contenuto della comunicazione.

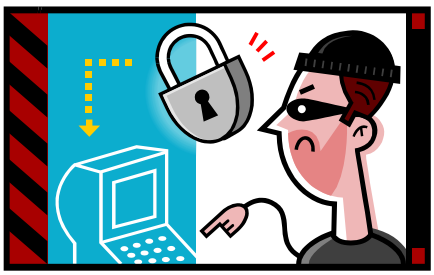
Questi certificati devono essere rilasciati da un certificate authority o comunque da un sistema che accerta la validità dello stesso in modo da definire la vera identità del possessore (i browser web sono creati in modo da poter verificare la loro validità tramite una lista preimpostata).

La password

La password protegge la tua Privacy, previene intrusioni e mette al sicuro i dati ! Per questo occorre che sia sicura e che venga cambiata periodicamente.

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)



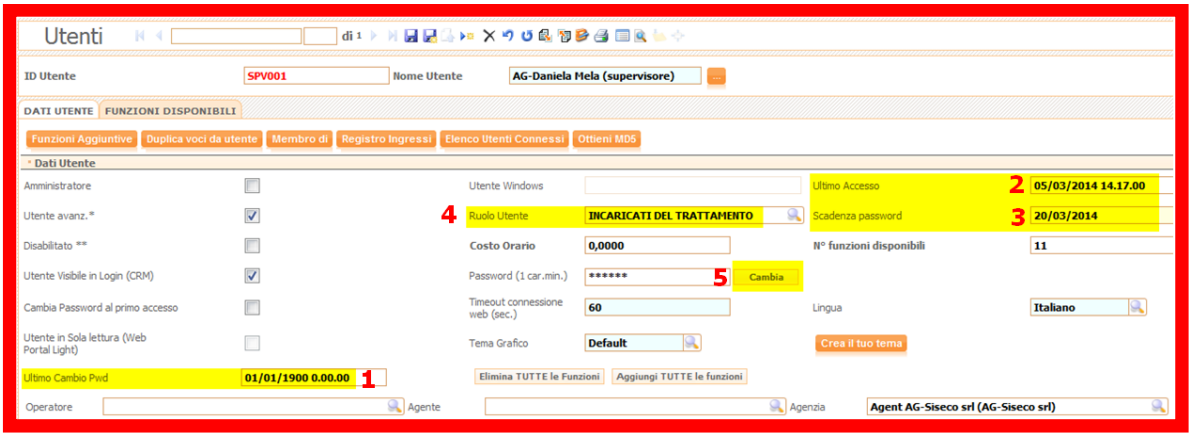
Impostare la password nel CRM

Oltre alla password nativa del PC utilizzato, per il rispetto della Privacy, il CRM adotta una propria gestione delle password che secondo quanto previsto dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del D.Lgs 196/03 allegato "B").

La password "standard" del CRM è **12345Aa!** e **va cambiata al primo accesso al sistema.**
Ricordate sempre che la password ha un ruolo importante per la sicurezza dei dati e dell'azienda!

Vediamo alcuni aspetti che si possono collegare facilmente all'uso quotidiano e pratico del CRM.
Accendendo al CRM nel menù Gestione Utenti è possibile visualizzare quando è stato fatta

- l'ultima modifica della password (1),
- L'ultimo accesso nel CRM (2),
- La scadenza della password (3)
- Il ruolo dell'utente nel "trattamento dei dati" nel caso sia coinvolto (4).



Tipologie di ruoli per la privacy nel decreto legislativo 30 giugno 2003, n. 196:

- **Titolare del trattamento:** è la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento dei dati personali ed agli strumenti utilizzati, ivi compreso il profilo della sicurezza
- **Responsabile del trattamento:** è la persona fisica, giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento dei dati personali.
- **Incaricati del trattamento:** è la persona fisica autorizzata a compiere le operazioni di trattamento dal titolare o dal responsabile. L'art. 30 del Codice precisa che le operazioni di trattamento possono essere compiute solo da soggetti nominati incaricati. Tale specificazione rende doverosa la designazione all'interno della struttura del titolare.

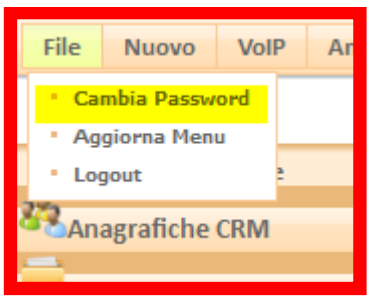
Cambio della password nel CRM

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)

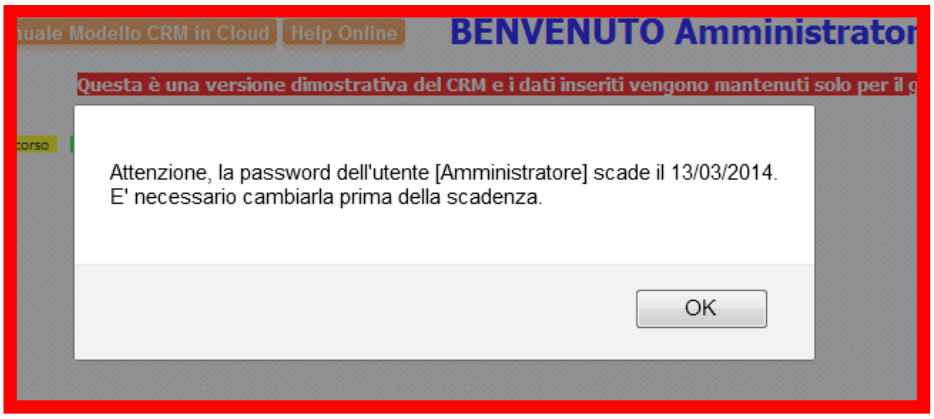
Non è necessario che l'amministratore conosca la vecchia password dell'utente in quanto questa non viene richiesta dal CRM per effettuare l'aggiornamento.

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

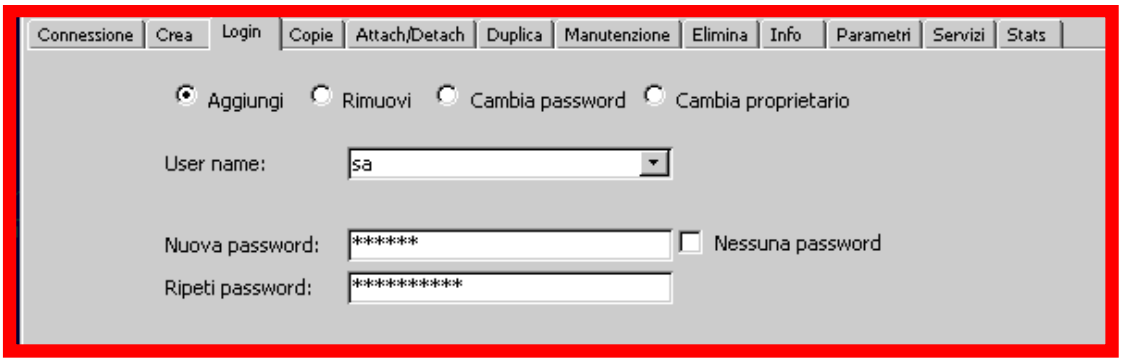
In caso di modifica da parte dell'**utente** stesso, è sufficiente entrare nel menu file in alto a sinistra nella Home Page o cliccare sul nome dell'utente connesso visualizzato in alto a destra:



Infine, sulla maschera principale subito dopo il login viene indicato quanti giorni mancano al cambio della password:



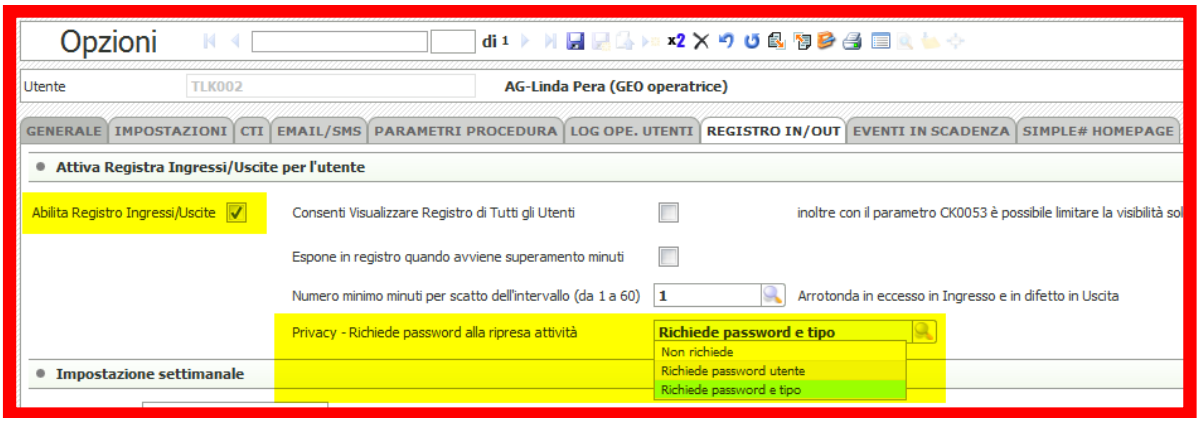
Oltre alle password di accesso nel CRM esiste anche la password di sicurezza per il collegamento a **SQL**, che consigliamo vivamente di non lasciare **mai vuota**.
Di norma quando viene installato il motore **MSDE** sul server la password **non viene definita**. Può comunque essere **inserita velocemente** in seguito utilizzando le funzioni presenti in Utilità / Gestione Database Server nella linguetta "LOGIN".



Gestione delle Pause Operatore

Il CRM rende disponibile all'operatore un tasto Pausa con cui notificare la sospensione temporanea dell'attività e bloccare contestualmente l'accesso al CRM.
Per la conformità alla Privacy durante le pause delle attività dell'operatore, in cui la postazione rimane non presidiata, occorre agire nelle "Opzioni" dell'utente (Utilità / Opzioni, sul TAB "Registro In/Out") è abilitare il registro Ingressi/Uscite ed impostare la richiesta 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. Non conforme alla Privacy.
- **Richiede password utente:** quando l'operatore torna dalla pausa deve inserire la propria password per poter riprendere l'attività.
- **Richiede password e tipo:** come sopra ma permette l'inserimento motivo (da una lista preimpostata) per cui la pausa è stata effettuata.



Parametri per la gestione password

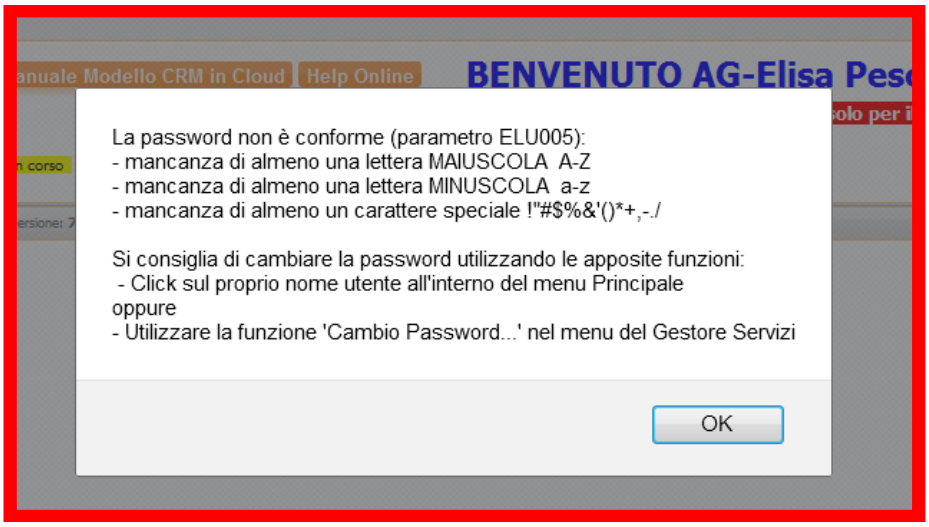
Nel menu Utilità, alla voce "Parametri della Procedura", abbiamo a disposizione dei parametri specifici per la gestione e la modifica "obbligatoria" delle password.

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: impedisci 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 il CRM dovesse rilevare che alcuni utenti posseggono una password non conforme, avviserà l'utente con un messaggio simile al seguente:



I sistemi operativi Windows98, Windows98SE ed inferiori non possiedono i requisiti di sicurezza previsti dalla legge.
Ricordiamo che Microsoft non rilascerà più alcun supporto tecnico dal:

- 11 luglio 2006 per i sistemi **Windows 98, Windows 98 SE** e **Windows Millennium Edition (Me)**.
- 8 aprile 2014 per i sistemi **Windows XP**

Pertanto 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.

In tali situazione è opportuno riferirsi al commerciale impresoft di riferimento per individuare un percorso di adeguamento alla sicurezza di tutta la soluzione installata:

- Piattaforma Windows e prerequisiti applicazioni, CRM, Centralino VoIP, Predictive lato server
- Browser e Client VoIP lato Client.

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 nel 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 archiviarle 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**.
- **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&C0]!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 cosi più facili da ricordare. Ad esempio:

- (!Sì 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.

Si ricorda che oltre alla gestione password del CRM è disponibile la gestione password del PC, per cambiarla è sufficiente premere:
CTRL + ALT + CANC e scegliere la voce "cambia password"

3. Sicurezza nel Servizio CRM

Continuità del servizio CRM in Cloud

- **Up-time del servizio, dichiarato dal fornitore della componente IAAS è pari al** 99%, 24h x 7 gg.
- **Backup dati**: salvataggio periodico dei file che compongono il sito in modo che siano sempre a disposizione in formato digitale le informazioni nel caso in cui vengano in qualche modo perse o cancellate.
- **Monitoraggio 24h su 24h**: i server hanno un sistema di allarme 24h su 24h collegato con i tecnici che segnala il possibile problema. Il check sulla macchina avviene ogni minuto.
- **Aggiornamenti software CRM di base**: vengono effettuati da impresoft aggiornamenti costanti del sistema operativo e più in generale della parte software del server.
- **Gruppo di continuità**: consente il funzionamento del server anche nel caso in cui venga a mancare la corrente elettrica.
- **Architettura del servizio**: l'architettura è modulare e distribuita su più server applicativi, frontend, database e voce. Viene utilizzata la piattaforma Windows Server e database Microsoft SQL Server con componenti software certificati.
- **Server farm**: le macchine sono fisicamente collocate presso server farm **Italiana** che mettono a disposizione la propria sala dati garantendo condizioni di massima sicurezza, tra cui dispositivi di controllo incendi, dispositivi antiallagamento, condizionamento dell'aria, Uninterruptable Power Supply, controllo e registrazione di tutti gli accessi. La connettività è diretta verso il MIX di Milano ed è ridondata con più carrier, per la massima continuità del servizio.
- **Firewall**: è un'ottima protezione lato server che chiude definitivamente l'accesso dall'esterno di alcune porte del sistema. Tutti gli accessi extra rispetto ai protocolli http dovranno essere esplicitamente richiesti ed autorizzati
- **Controlli sugli utenti**: vengono utilizzati tutti gli accorgimenti base e più comuni per evitare che possa entrare nel sistema un esterno (lunghezza e gestione password,...). L'unico che ha la possibilità di operare a 360° sul server è l'amministratore di sistema.

La raggiungibilità del servizio in CLOUD, sia come BMG (Banda minima garantita) che come disponibiità è a carico del cliente.

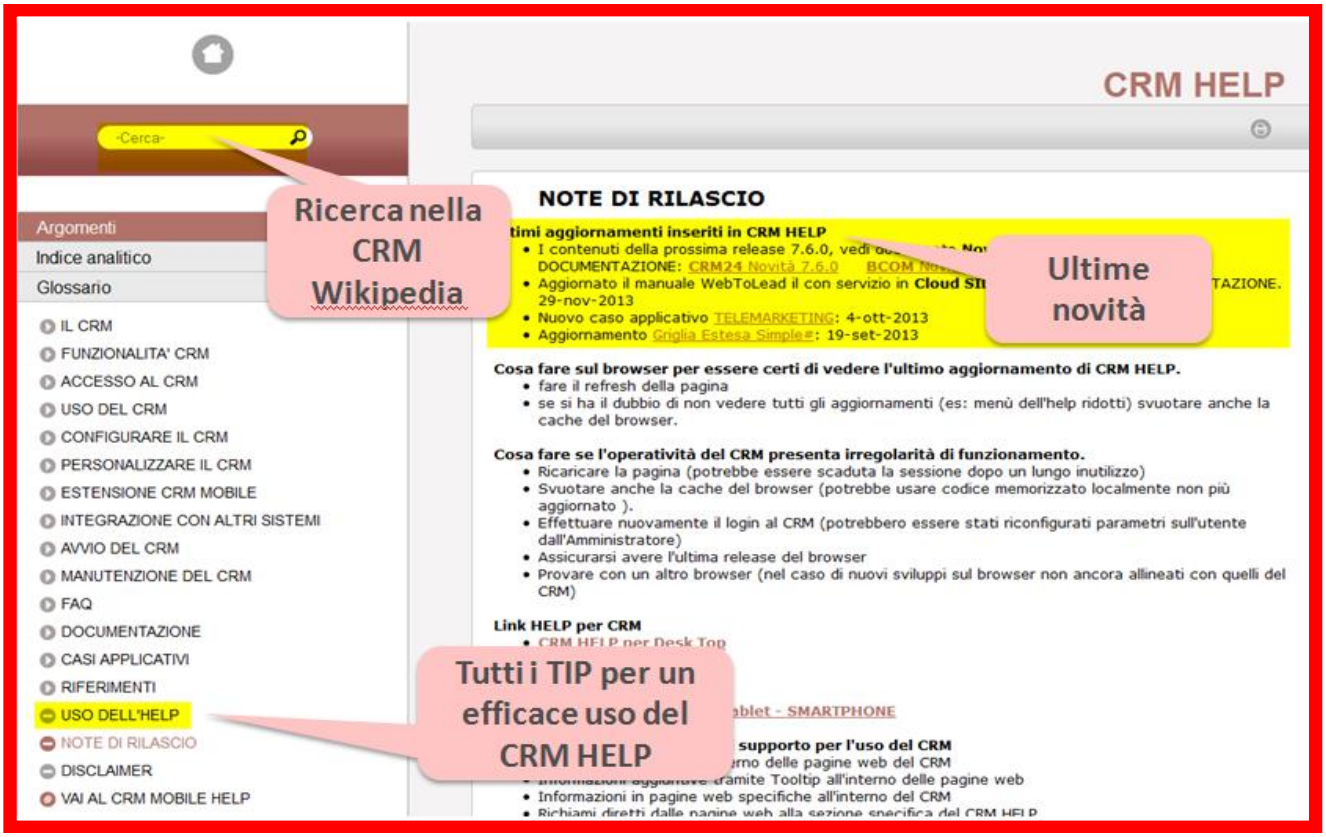
Assistenza e Supporto on line

Nel caso accidentale di problemi sul servizio CRM è disponibile il servizio help desk (Tel. +39-0331-9351 Post 2) sia per:

- Gestione software: con personale tecnico e commerciale a supporto del cliente sempre presente negli orari d'ufficio per soddisfare ogni tipo di richiesta dal ripristino all'ampliamento di funzioni. Il livello e la forma di assistenza è definito da un apposito contratto di Service Level Agreement (SLA).
- Guasto Hardware: il nostro personale tecnico effettuerà in tempo reale un intervento di 1° livello nel caso di rottura hardware del server. E' disponibile inoltre una macchina ridondata in grado di entrare in funzione in sostituzione di quella guasta.

Note: L'eventuale ripristino di un backup antecedente, a seguito di errori commessi dall'utente, non è compreso nel servizio di assistenza.

Oltre al servizio Help Desk, tutte le funzioni del CRM e la libreria della documentazione, questo manuale incluso, sono presenti sull'**HELP on Line** all'indirizzo:
http://intranet.siseco.it/crmhelp/CRM_HELP.htm
All'interno vi è un dettagliato menù ed è disponibile il tasto **cerca** con cui è possibile individuare velocemente la sezione di interesse semplicemente digitando il nome della funzione ricercata.



Per una maggiore comprensione delle logiche di funzionamento e personalizzazione del CRM si rimanda alle specifiche sezioni del manuale **Guida Rapida all'uso,**si scarica dal menù ? del CRM, di cui si consiglia una lettura completa.

La Sicurezza nelle funzioni del CRM

Nel riepilogare alcune delle principali funzioni del CRM, si evidenziando gli aspetti per la gestione della privacy in funzione dei livelli di visibilità che ciascun utente ha impostati per il ruolo ricoperto.

- **Gestione Privacy** attraverso l'applicazione dei processi standard ISO 27001.
- Home page del CRM, **personalizzabile per il profilo**, sintetizza l'andamento delle attività in ottica commerciale ed operativa, finalizzata ad avere sempre un quadro della situazione.
- Gestione automatica di "n" meccanismi di notifica ed alert **per lo specifico profilo** tramite email (notifica scadenza, cambio di stato pratica, sollecito documentazione, memo appuntamenti, avvenuta delibera, ecc…).
- Gestione delle anagrafiche e delle autorizzazioni di accesso e operative di ogni utente **a seconda del ruolo e della gerarchia.**
- Gestione di appuntamenti, opportunità, offerte/ordini (pratiche) legate a ciascuna anagrafica in **funzione della finalità.**
- Gestione delle email in entrata e uscita correlate all'anagrafica (**solo per quelle a cui si ha accesso**).
- Gestione stampa preventivi, richieste documenti, lettere di presentazione **personalizzate**.
- Gestione della governance dei processi e della produttività, gestisce report sulle performance degli utenti, delle funzioni e dell'azienda, e verifica gli accessi operativi in conformità **al work flow definito e ai ruoli impostati.**
- **Gestione del tracciamento di tutte le attività svolte** su ogni anagrafica/opportunità registrando l'utente, il giorno e l'ora dell'attività.
- Gestisce soluzioni ad hoc per implementare il processo del cliente tramite semplici ed efficaci funzioni di personalizzazione del CRM.

Le funzioni di Controllo nel CRM

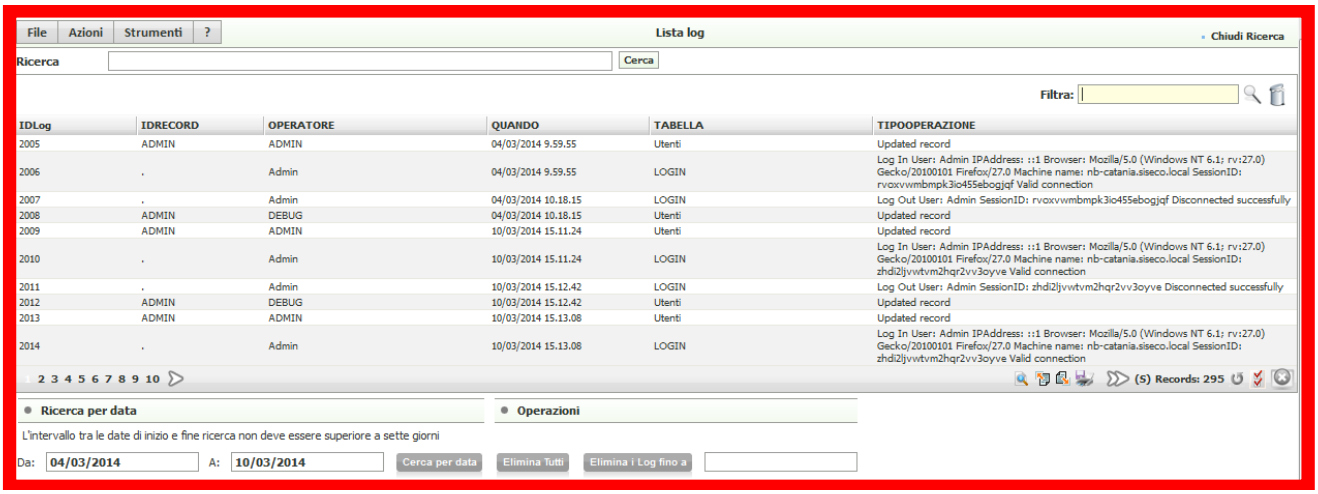
Le funzioni di controllo permettono di accedere al tracciamento delle attività che sono state fatte nel CRM per individuare accessi anomali o a rischio. Vi sono tracciamenti di base sempre attivi che possono essere ampliati per avere tracciamenti specifici per ogni attività svolta nel CRM.

LOG delle Operazioni

Nel menù Amministrazione la voce **Log delle Operazioni Utente** vengono registrati la maggior parte degli eventi che si sono verificati durante l'utilizzo del CRM. Nel log possiamo trovare:

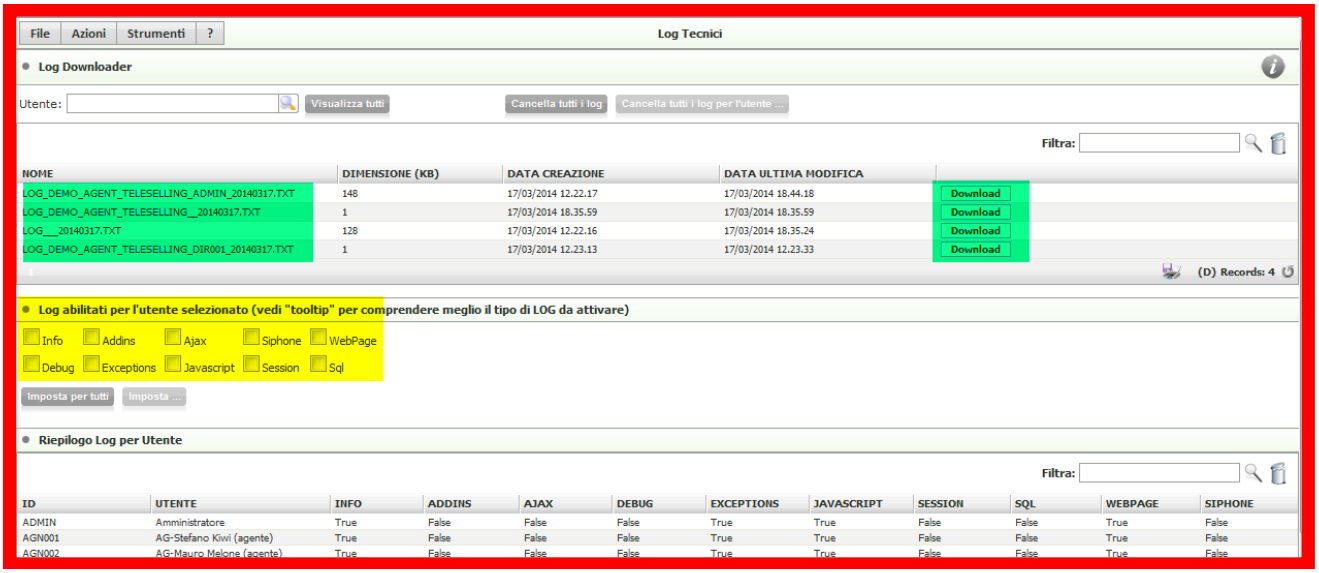
- le informazioni relative agli EXPORT effettuati, indicando l'utente che ha eseguito l'operazione, il formato utilizzato, data ed ora dell'export.
- gli accessi di tutti gli operatori e le tabelle e il tipo di operazione svolto.

Il Log non è modificabile dall'utente e si genera automaticamente senza intervento degli utenti.

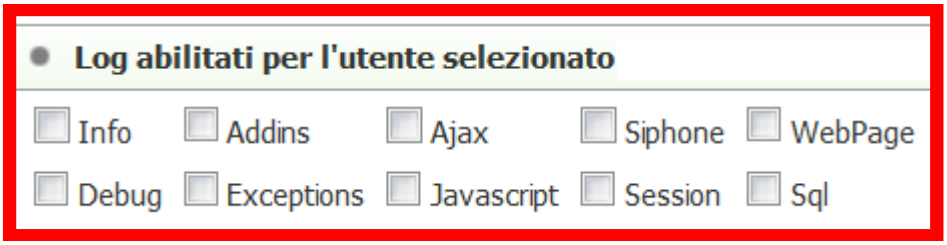


LOG Tecnici

A livello di controllo più profondo sulle attività svolte usando il CRM è disponibile nel menù **Amministrazione** - **Log Tecnici** il tracciamento di tutte le attività svolte.



Possono essere attività log per singolo utente e per singola tipologia di eventi:



E con il tasto donwload scaricare il TXT di tutte le operazioni effettuate.

Il servizio commerciale è a disposizione per fornire il supporto per l'indagine degli eventi non desiderati nel tracciamento raccolto.

I Log Tecnici sono utili anche in presenza per l'indagine di comportamenti del CRM non secondo le attese, in questo caso l'Assistenza Tecnica impresoft darà le istruzioni su come effettuare il Log Tecnico.

Controllo nei Workflow

Oltre ai limiti di visibilità impostati secondo il ruolo degli utenti è possibile avere ulteriori limitazioni in sul workflow dei processi realizzati; per esempio:

- Funzioni bloccanti (esempio: se non hai fatto firmare l'autorizzazione al trattamento dati non vai avanti – se non hai consegnato la documentazione richiesta non vai avanti ...)
- Stati Opportunità/Ordini/Pratica bloccanti per livelli di gerarchia (validazione pratiche)
- Blocco di visibilità su informazioni in funzione degli stati di avanzamento….

4. Sicurezza nel Servizio VoIP

Vulnerabilità nella telefonia VoIP

L'utilizzo delle nuove tecnologie VoIP nei centralini aziendali e del call center apre una fronte di vulnerabilità completamente nuovo per gli addetti al servizio.
L'unificazione del traffico voce e dati all'interno di un'unica infrastruttura VoIP comporta problemi legati alla sicurezza che con i centralini tradizionali non erano presenti e che sono ampiamente noti nel mondo dati.

I clienti talvolta rilevano tentativi fraudolenti di accedere alla propria rete telefonica VoIP, in alcuni casi questi attacchi hanno successo. Questo può comportare la generazione di traffico anomalo e quindi ad una bolletta telefonica eccessiva. Anche un singolo episodio di hacking telefonico può lasciare comportare un notevole esborso economico.

Considerando l'importanza che il centralino IphoneBox riveste per il business del cliente occorre rilevare come anche la sicurezza informatica e la protezione del sistema telefonico sia FONDAMENTALE.

Anche in quest'ambito impresoft interviene verso i propri clienti indicando linee guida e gli strumenti per proteggere il centralino VoIP, che sia parte o meno di una soluzione CRM, ed offre la sua consulenza e esperienza per la prevenzione delle frodi sul traffico voce e per il rispetto della privacy nell'uso del centralino VoIP. In questo contesto oltre ad applicare gli accorgimenti di sicurezza visti nei paragrafi precedenti occorre contrastare gli ulteriori pericoli legati alle frodi sul traffico voce, allo scopo ad ogni aggiornamento, della piattaforma VoIP IPhoneBox, vengono aggiunte nuove funzionalità per ridurre al massimo la probabilità di phone hacking.

Linee guida per la sicurezza VoIP

Il primo passo verso la messa in sicurezza della propria piattaforma VoIP passa per l'aggiornamento della release. Se si utilizza una versione di IphoneBox precedente alla 4.6.x e le impostazioni di sicurezza (password) sono le stesse da molto tempo si consiglia vivamente di AGGIORNARE IL SISTEMA all'ultima versione e cambiare le password utilizzando le regole viste per le password del CRM.
In particolare, le versioni più recenti del software consentono di monitorare l'accesso fraudolento e bloccare i tentativi non autorizzati da IP selezionati.

ATTENZIONE: avvisate l'Assistenza impresoft sugli interventi di aggiornamento effettuati affinché il processo di eventuale teleassistenza resti efficace e rapido.

Si suggerisce inoltre di chiedere all'amministratore ICT di adottare le seguenti linee guida di sicurezza:

- Assicurarsi che sia attivo un firewall sulla LAN e limitare il traffico TCP e UDP porta 3541, evitando che le altre porte del router siano aperte inutilmente. Quando le porte del firewall sono aperte dovrebbero consentire solo il traffico da e verso indirizzi IP noti.
- Gli utenti remoti dovrebbero accedere a queste porte esclusivamente tramite VPN oppure tramite l'accesso NAT da indirizzi IP statici e noti
- Verificare che il Firewall sia in grado di bloccare le attività sospette su una qualsiasi delle porte esterne (UDP e TCP)
- Installare il software Antivirus a livello business su tutti i PC della rete
- Tutte le password devono essere cambiate regolarmente e generate casualmente (si veda il paragrafo sull'uso delle password)
- Limitare l'accesso all'interfaccia di amministrazione WEB
- Assicurarsi che i provider della linea telefonica (ISDN , analogiche , VoIP) controllino regolarmente il traffico e implementino algoritmi anti- frode. **Ove possibile si dovrebbe anche comunicare al provider un limite massimo per la spesa telefonica quotidiana.**

A supporto dell'utilizzo in sicurezza del centralino VoIP è possibile accedere alla seguente documentazione on line:

- http://www.voispeed.com/man/platform/it/46/manuale.htm

5. Conclusioni

Abbiamo visto come la gestione della Privacy e della Security non sia solo questione di prodotto ma di procedure e processi che coinvolgono sia il fornitore della soluzione CRM e il Cliente con i suoi addetti per il suo utilizzo. I punti rilevanti di questa filiera sono i seguenti:

- impresoft srl, è certificata ISO 9001, nell'ambito delle procedure di progettazione, sviluppo, installazione, integrazione ed assistenza di piattaforme software evolute per la gestione di CRM, Multimedia Contact Center e sistemi CTI.

- impresoft srl per garantire la selezione di controlli di sicurezza adeguati e proporzionati, adotta lo standard ISO 27001 relativamente al ISMS (Sistema di Gestione della Sicurezza delle Informazioni.

- Il CRM BCOM di impresoft, completato dalla soluzione IPHONE BOX – VOIP, per la gestione delle chiamate entranti e uscenti, e dal modulo Predictive per la gestione automatica delle chiamate uscenti, incorpora tutti gli elementi per:
  - essere conforme alla Privacy dei dati trattati
  - la sicurezza dell'accesso agli stessi e della piattaforma.

  Rilevante è anche la flessibilità del CRM di garantire visibilità diversificate sulle informazioni gestite in funzione del profilo dell'utente connesso.

- Il Cliente che, mettendo in atto le procedure di privacy corrette, ha a disposizione una soluzione CRM e il partner impresoft per implementare correttamente i processi nel rispetto delle norme in essere e in tutta sicurezza.

Ovviamente in questa filiera è necessario inserire anche l'Operatore di rete sia per la banda internet che per le soluzioni in cloud. Anche su questi aspetti impresoft è presente con proprie proposte per coprire ogni esigenza necessaria per la soluzione che si intende realizzare.

Buon lavoro in tutta Privacy e Security !

Il team di Produzione