Programma LibSvi	Procedura *Gestione della sicurezza nell'accesso ai dati dei portali/applicativi delle librerie dello Studio Filippo Albertini*

La libera professione oggetto del presente documento viene svolta con riferimento alla Legge n. 4 del 14 Gennaio 2013.

Studio Filippo Albertini Via Euclide, 7 - 47841 Cattolica (RN) Cell. 347/7163264 Fax 0541/0531186
Web www.filippoalbertini.it E-Mail filippo@filippoalbertini.it PEC filippo.albertini@pec.it
Cod. Fisc. LBRFPP68M23C357N P.Iva 01881570400 - Attività svolta ex legge n. 4/2013

Indice

Studio Filippo Albertini Via Euclide, 7 - 47841 Cattolica (RN) Cell. 347/7163264 Fax 0541/0531186
Web www.filippoalbertini.it E-Mail filippo@filippoalbertini.it PEC filippo.albertini@pec.it
Cod. Fisc. LBRFPP68M23C357N P.Iva 01881570400 - Attività svolta ex legge n. 4/2013

Sicurezza nell'accesso ai dati (new)

Accesso

Per entrare nelle procedura è necessario conoscere il codice utente e la password.

Profilazione

Ogni utente può accedere alle sole funzionalità che gli sono state autorizzate.
E' possibile assegnare all'utente o uno più gruppi; ad ogni gruppo sono assegnate le funzioni abilitate.
E' anche possibile assegnare direttamente le funzioni all'utente.

Ogni singola funzionalità è identificata univocamente con un codice che viene poi richiamato nelle profilazioni potendo indicare anche le opzioni, eventualmente gestite.

Scadenza password

In rispetto alle normative sulla protezione e sicurezza dei dati ogni 180 giorni la password scade e l'utente al momento dell'accesso alla procedura è costretto a digitare la nuova password.

Tramite il parametro di sistema PASSWORD.GIORNI.SCADENZA è possibile indicare il numero di giorni che devono passare dopo i quali la password scade ed è quindi necessario cambiare la password; il valore predefinito è 180

Nella pagina che si apre dopo aver fatto il login (pagina Main) viene visualizzato un messaggio all'utente se la password è in scadenza; il parametro di sistema GIORNI.PREAVVISO.SCADENZA.PASSWORD indica quanti giorni prima iniziare ad avvisare l'utente che la password sta per scadere (default 20).

Cambio password

La nuova password indicata non può essere uguale alla precedente.

E' anche possibile, tramite il parametro generale CHECK.LAST.RECENTLY.PASSWORD, impedire che l'utente abbia inserito una delle N password precedenti. All'interno del database non vengono salvate le password inserite dall'utente, ma l'MD5 delle password.

Autenticazione da dominio

E' possibile abilitare l'autenticazione degli utenti utilizzando le password presenti nel dominio di rete (Web.Config → DominioActiveDirectory).

Studio Filippo Albertini Via Euclide, 7 - 47841 Cattolica (RN) Cell. 347/7163264 Fax 0541/0531186
Web www.filippoalbertini.it E-Mail filippo@filippoalbertini.it PEC filippo.albertini@pec.it
Cod. Fisc. LBRFPP68M23C357N P.Iva 01881570400 - Attività svolta ex legge n. 4/2013

In questa modalità ogni utente applicativo è associato ad un utente di dominio di rete e l'autenticazione viene effettuata verificando la password dal dominio di rete.

E' anche possibile attivarlo tramite il parametro di sistema LOGIN.ACTIVE.DIRECTORY

Domanda segreta

Se l'impostazione di sistema è di richiedere la domanda di sicurezza, la prima volta che si prova a cambiare la password viene richiesta la domanda e risposta segrete.

Tramite il parametro di sistema PASSWORD.DOMANDA.SEGRETA è possibile indicare se richiedere all'utente la domanda segreta al momento del cambio password (default S, per disattivare mettere N)

Sicurezza password inserite

La password scelta dall'utente deve rispettare dei requisiti minimi di sicurezza.
Per ogni password viene calcolata la sua forza con un valore (tra 0 e 6) secondo questo algoritmo:

- + 1 punto se ha almeno 4 caratteri
- + 1 punto se ha almeno 12 caratteri
- + 1 punto se ha sia caratteri in maiuscolo e in minuscolo
- + 1 punto se contiene numeri
- + 1 punto se contiene caratteri speciali (ad esempio , ; @ # < >)
- + 1 punto se contiene almeno 4 caratteri differenti

Un parametro di sistema (PASSWORD.LENGTH) indica il numero minimo di caratteri accettati per la nuova password (default 8).

Un altro parametro di sistema (PASSWORD.MIN.STRENGTH) indica il livello minimo di sicurezza richiesto. Il livello default è 3.

Scadenza sessione

Nelle pagine web viene verificato se l'utente corrente ha fatto accesso nelle ultime 4 ore, verificando i login sulla tabella Eventi con l'indirizzo ip corrente. Se non è presente un login l'utente viene rimandato alla pagina iniziale di login.

La scadenza delle sessioni sui siti è impostata invece a livello di Web.Config ed è specifica di ogni portale.

Blocco utente

Dopo 6 mesi di inutilizzo di un utente questo viene automaticamente bloccato, ovvero l'utente non è più utilizzabile per accedere alla procedura finché l'amministratore non ne effettua lo sblocco.

Studio Filippo Albertini Via Euclide, 7 - 47841 Cattolica (RN) Cell. 347/7163264 Fax 0541/0531186
Web www.filippoalbertini.it E-Mail filippo@filippoalbertini.it PEC filippo.albertini@pec.it
Cod. Fisc. LBRFPP68M23C357N P.Iva 01881570400 - Attività svolta ex legge n. 4/2013

Tramite il parametro di sistema PASSWORD.GIORNI.INUTILIZZO.BLOCCO si indica il numero di giorni che devono passare senza essere mai acceduti alla procedura, dopo i quali l'utente viene bloccato; il valore predefinito è 180 giorni.

L'utente viene bloccato quando viene indicata una password errata per un certo numero di volte; il parametro di sistema TENTATIVI.FALLITI.LOGIN.ACCETTATI indica quante volte può l'utente sbagliare in 5 minuti la password prima che in automatico gli sia bloccato l'utente. Il valore di default è 10 (10 password errate consecutive in 5 minuti).

Quando gli utenti sono bloccati non possono più accedere alla procedura, fino a quando un utente amministratore lo sblocca. Se l'utente non viene mai utilizzato nei 5 giorni successivi allo sblocco viene bloccato un'altra volta.

Blocco accesso per ip

E' possibile bloccare l'accesso ad una serie di indirizzi ip specifici, indicandoli dentro una tabella (TABE_IPB).

Se è valorizzato il parametro di sistema MAX.DISTINCT.USER.FOR.IP è possibile bloccare l'accesso alla procedura se sono stati effettuati troppi login con utenti differenti tutti dallo stesso indirizzo ip.

Visualizzazione password digitata

Di default 'utente non può visualizzare la password mentre la digita sulla pagina di login; tramite il parametro generale LOGIN.VIEW.PASSWORD è possibile abilitare un bottone sotto alla password, cliccato il quale si tolgono gli asterischi ed è possibile vedere la password mentre la si digita.

Impostazione automatica codice utente utilizzato in precedenza

Tramite il parametro generale COOKIE.LOGIN.CODICE.ACCESSO è possibile indicare se il portale deve memorizzare nei cookie il codice utente con cui si ha fatto accesso al portale l'ultima volta; in questo modo alla successiva apertura del portale viene valorizzato il codice utente utilizzato in precedenza.

Accesso con la password dell'amministratore

Ove abilitato è possibile accedere alla procedura ed entrare con qualunque utente indicando la password dell'amministratore; l'operazione viene registrata nella tabella delle sessioni.

Tramite il parametro di sistema WEB.LOGIN.ADMIN.PASS è possibile disabilitare questa modalità.

Accesso con password temporanea

Studio Filippo Albertini Via Euclide, 7 - 47841 Cattolica (RN) Cell. 347/7163264 Fax 0541/0531186
Web www.filippoalbertini.it E-Mail filippo@filippoalbertini.it PEC filippo.albertini@pec.it
Cod. Fisc. LBRFPP68M23C357N P.Iva 01881570400 - Attività svolta ex legge n. 4/2013

Per scopi amministrativi è possibile farsi rilasciare, dietro esplicita e formale richiesta, dallo Studio Albertini Filippo una password temporanea per l'accesso con qualunque profilo. Questa password viene generata ed è valida per entrare sul programma indicato solamente nella finestra temporale definita. Ogni accesso alla procedura con queste password temporanee viene registrato nella tabella delle sessioni (LogOnWithPasspartout).

E' possibile generare delle password temporanee in base alla società anziché ad un singolo utente: con queste password è possibile entrare con tutti gli utenti che sono della società per cui è stata creata la password temporanea.

Password di primo accesso

I nuovi utenti vengono creati con una password temporanea di primo accesso.
Al primo accesso dell'utente viene quindi richiesto il cambio password e non può entrare sul portale fino a che non ha impostato una nuova password personale.

Accesso non riuscito per password sbagliata

Quando si inserisce la password errata in automatico il portale invia un email all'utente, se ha l'email associata, per notificare il tentativo di accesso.

Tramite il parametro di sistema LOGIN.EMAIL.PASS.ERRATA è possibile disattivare queste notifiche.

Recupero password

Le password originali inserite dagli utenti non sono recuperabili perchè vengono archiviate per le verifiche di autenticazione in formato MD5 e confrontate con l'MD5 del valore inserito dall'utente.

In caso di dimenticanza della password è possibile richiedere ad un utente amministratore di reimpostare una nuova password di primo accesso.

Per i siti web l'utente può richiedere una nuova password temporanea di primo accesso, se ha indicato nel proprio profilo l'email e il codice fiscale. Dopo aver sbagliato la password è possibile cliccare su "Invio password di primo accesso" e viene richiesto il codice fiscale dell'utente; questa operazione invalida la password attualmente impostata nel portale e crea una nuova password temporanea di primo accesso, che viene inviata via email, all'indirizzo indicato nel profilo, all'utente.

Amministrazione utenti

Gli utenti del gruppo ADMINISTRATORS e l'utente codice 999 o 00999 sono gli utenti amministratori di sistema, che hanno accesso a tutte le funzionalità.

Studio Filippo Albertini Via Euclide, 7 - 47841 Cattolica (RN) Cell. 347/7163264 Fax 0541/0531186
Web www.filippoalbertini.it E-Mail filippo@filippoalbertini.it PEC filippo.albertini@pec.it
Cod. Fisc. LBRFPP68M23C357N P.Iva 01881570400 - Attività svolta ex legge n. 4/2013

Sui portali web è anche possibile assegnare ad alcuni utenti specifici la sola gestione degli utenti, dando le funzionalità [CODICE PROGRAMMA].USERS; ad esempio il gruppo GESTIONE può avere l'abilitazione SGD.USERS, e in questo modo tutti gli utenti che hanno questo gruppo possono gestire gli utenti sul sito SGD.

Sessioni, Log e Eventi

Tutte le operazioni eseguite dagli utenti vengono memorizzate sulla tabella Sessioni, Log ed Eventi.

Ogni accesso alla procedura crea una riga nella tabella delle Sessioni dove viene salvato:

- l'utente di dominio (UtenteDominio)
- l'utente applicativo (UtenteApplicativo)
- il nome del computer (Computer)
- la data del login (Logon)
- l'ultima volta che ha usato la procedura (LastOnline)
- la data del logout (Logout)
- se ha fatto accesso tramite una password generata (LogonWithPasspartout)
- l'indirizzo ip (Ip)
- alcune informazioni relative al browser in uso (Informazioni)
- mac address (MacAddress)
- id del processo di Windows che esegue la procedura o portale (ProcessId)

La tabella degli Eventi memorizza le operazioni effettuate, le pagine del portale visitate e altri eventi tracciati a livello di procedura (consultazioni, etc).

La tabella _Log memorizza le attività (informazioni, errori, …) gestite dalla procedura.

Tracciabilità del dato

Dove abilitato tramite strumenti automatici del database (trigger) vengono tracciate le modifiche a livello di inserimento, cancellazione e modifica (prima e dopo) con riferimenti all'utente e alla sessione (tabelle _Storico).

Studio Filippo Albertini Via Euclide, 7 - 47841 Cattolica (RN) Cell. 347/7163264 Fax 0541/0531186
Web www.filippoalbertini.it E-Mail filippo@filippoalbertini.it PEC filippo.albertini@pec.it
Cod. Fisc. LBRFPP68M23C357N P.Iva 01881570400 - Attività svolta ex legge n. 4/2013

Allegati

Riepilogo parametri

Tipo	Nome
Generale	CHECK.LAST.RECENTLY.PASSWORD
Generale	COOKIE.LOGIN.CODICE.ACCESSO
Sistema	GIORNI.PREAVVISO.SCADENZA.PASSWORD
Sistema	LOGIN.ACTIVE.DIRECTORY
Sistema	LOGIN.EMAIL.PASS.ERRATA
Generale	LOGIN.VIEW.PASSWORD
Sistema	MAX.DISTINCT.USER.FOR.IP
Sistema	PASSWORD.DOMANDA.SEGRETA
Sistema	PASSWORD.GIORNI.INUTILIZZO.BLOCCO
Sistema	PASSWORD.GIORNI.SCADENZA
Sistema	PASSWORD.LENGTH
Sistema	PASSWORD.MIN.STRENGTH
Sistema	TENTATIVI.FALLITI.LOGIN.ACCETTATI
Sistema	WEB.LOGIN.ADMIN.PASS

Firmato da:
MANCINI PAOLA
Motivo:

Data: 29/12/2017 13:35:10

Studio Filippo Albertini Via Euclide, 7 - 47841 Cattolica (RN) Cell. 347/7163264 Fax 0541/0531186
Web www.filippoalbertini.it E-Mail filippo@filippoalbertini.it PEC filippo.albertini@pec.it
Cod. Fisc. LBRFPP68M23C357N P.Iva 01881570400 - Attività svolta ex legge n. 4/2013