MISURE DI SICUREZZA PER GLI UTENTI E PER LE APPLICAZIONI

Banche Dati

L'accesso alle banche dati del sistema BDPI/TOSCA oggetto dell'incarico di migrazione e del nuovo sistema M.A.R.T.E. è limitato a un certo numero di utenti della PO Risorse Dati, Open Data, SIT in possesso delle autorizzazioni di incaricati al trattamento dati personali e amministratori di sistema.
Tale meccanismo sarà esteso anche al fornitore per la durata del contratto, con analoghe credenziali nominative, che dovrà quindi avere le opportune nomine per il trattamento.
Si fa notare che la password di amministratore totale della banca dati è ad esclusivo appannaggio del DBA dell'unità sistemi della Direzione Sistemi Informativi del Comune di Firenze.

VPN e macchine

Verrà creata una vpn o più vpn ad hoc con accesso consentito solo alle macchine necessarie allo svolgimento delle attività, seguendo il criterio del "privilegio minimo".
L'accesso alla vpn avviene tramite **credenziali di dominio** che saranno create in modo nominativo e valevoli per la durata del contratto.
Per l'accesso in ssh alle macchine che ospitano i sistemi, verranno analizzati i requisiti di necessari allo svolgimento delle attività e create le opportune credenziali potenziate sulla macchina. L'abbinamento al nominativo è comunque garantito tramite il doppio accesso basato sia su credenziali di dominio e credenziali per eventuale accesso potenziato.

RDEXplorer/SUITE

L'applicativo per la navigazione dei dati della BDPI denominato RDExplorer/Suite è ad accesso limitato ad utenti che ne fanno richiesta tramite il loro dirigente/delegato privacy. Tale sistema è accessibile tramite il meccanismo di SSO dell'ente che si basa sugli utenti di dominio: il fornitore utilizzerà quindi le stesse credenziali create hoc per le altre necessità.
Si evidenzia che nel sistema è presente un meccanismo traccia le attivitàdell'utente, ne monitora il numero di richieste massimo che può essere fatto, e i giorni che passano dall'inutilizzo del sistema. Un utente che non accede al sistema per 180 giorni, viene disabilitato automaticamente e gli viene notificata via email tale disabilitazione. RDExplorer/Suite viene erogata via https, accessibile solo da intranet e implementa i normali meccanismi per la sicurezza delle Web Application. Per le utenze ad altre applicazioni (ove utilizzabili) saranno utilizzate le credenzali di dominio per poter accedere tramite Sistema Single Sign On.

Delta informativi

Verranno individuate delle misure in linea con quanto sopra quando se ne porrà l'esigenza. L'idea è di fare a livello di DB credenziali nominative a scadenza, mentre per eventuale accesso a macchine verranno utilizzate le credenziali di dominio e eventuale meccanismo in doppia autenticazione.

Si ricorda che le misure di sicurezza sono in costante miglioramento e potrebbero essere oggetto quindi di cambiamento.

Firmato digitalmente da:Piero Rossini
Data:04/03/2020 09:26:10

VANNUCCINI GIANLUCA
03.03.2020 10:13:07 UTC