UNIONE EUROPEA
Iniziativa a favore dell'Occupazione Giovanile
Fondo Sociale Europeo
Investiamo nel tuo futuro

garanzia giovani

ANPAL
Agenzia Nazionale Politiche Attive del Lavoro

PROCEDURA PER IL MONITORAGGIO DEL PROGRAMMA OPERATIVO NAZIONALE INIZIATIVA OCCUPAZIONE GIOVANI

ALLEGATO 3

SICUREZZA E QUALITÀ DATI IN SIGMA$_{GIOVANI}$

SOMMARIO

Introduzione

Il presente documento ha lo scopo di esporre, relativamente al sistema informativo di gestione del PON YEI, "SIGMA$_{Giovani}$", gli aspetti correlati alla qualità e sicurezza dei dati trattati.

In particolare, vengono descritte le modalità di raccolta dei dati, l'archiviazione dei dati, la trasmissione di dati, la sicurezza degli accessi.

1. La raccolta dati

In SIGMA$_{Giovani}$ la completezza della raccolta dei dati è implementata mediante appositi controlli e vincoli di obbligatorietà che, a seconda della forma di inserimento utilizzata (inserimento manuale o caricamento automatico), segnalano la mancanza del dato in modo interattivo o tramite rapporti di esecuzione.

Nel caso di inserimento da maschera la segnalazione, se vi è un vincolo di obbligatorietà, è bloccante. In questo caso le verifiche vengono effettuate tramite apposite funzionalità automatiche di controllo a livello di interfaccia (qualora il vincolo di obbligatorietà possa essere soddisfatto e circoscritto alla maschera) o tramite controlli in banca dati (qualora il vincolo di obbligatorietà sia condizionato alla presenza di informazioni già registrate in banca dati).

L'obbligatorietà dei campi sulle maschere è segnalata tramite un asterisco rosso e delle note esplicative.

Nel caso di caricamento automatico, i record che non soddisfano i requisiti di obbligatorietà (verificati tramite un processo di controllo automatico in background) vengono scartati, e segnalati nel rapporto di caricamento. Tipicamente l'organismo intermedio provvede all'analisi degli scarti, corregge o completa l'informazione e riesegue il caricamento dei soli record scartati.

Per i caricamenti tramite file l'obbligatorietà ed il formato dei dati sono riportati sul documento Protocollo di Colloquio disponibile sul portale SIGMAGiovani.

Il processo di controllo raccolta dati, da un punto di vista strettamente informatico, è caratterizzato dalla gestione dell'obbligatorietà mediante l'analisi di in appositi attributi del campo in modo da rendere parametrica e centralizzata la funzionalità di controllo.

2. Archiviazione

SIGMA$_{Giovani}$ dispone di un sistema centralizzato unico per l'archiviazione dei dati basato su di RDBMS SqlServer.

Il database viene salvato ad intervalli regolari nel corso della giornata tramite una procedura di backup incrementale, che salvaguarda l'integrità del database su base giornaliera.

Viene inoltre eseguito un ulteriore backup giornaliero durante la fascia notturna che salvaguarda l'integrità del database nel tempo permettendo anche di poter verificare i dati ad una data specifica.

I vincoli di integrità referenziale sono definiti in fase di progettazione del Database, mediante l'impostazione delle chiavi esterne (foreign keys) e dei vincoli (constraints).

In fase di esecuzione delle singole funzioni di inserimento/modifica, l'integrità e la consistenza dell'informazione viene assicurata nel seguente modo:

- blocco temporaneo del record logico oggetto della modifica. Se il sistema sta scrivendo l'informazione, il record non viene reso disponibile per una eventuale scrittura concomitante da parte di un altro utente che potrebbe alterarne il valore.
- dalla strutturazione delle operazioni di scrittura in transazioni logiche. La banca dati è di tipo relazionale ed è stata progettata seguendo le regole di normalizzazione. Frequentemente un'operazione di salvataggio coinvolge più tabelle. Qualora un'operazione di scrittura non dovesse terminare correttamente per un qualsiasi motivo, la strutturazione in transazioni garantisce che tutto il blocco di operazioni correlate venga o eseguito (e quindi consolidato mediante una operazione di "commit") oppure scartato ripristinando i valori precedenti (mediante un'operazione di "roll-back").

3. Registrazione delle operazioni e trasmissione dati

Tutte le operazioni di inserimento, modifica o cancellazione vengono registrate conservando l'identificativo univoco dell'autore dell'operazione, la data e l'operazione eseguita.

Si mette in evidenza che la tracciabilità dell'operazione è estesa a tutte le funzioni del sistema informativo e che vengono conservate tutte le registrazioni.

Viene così fornita la possibilità di risalire alla singola operazione ed all'autore, in modo da consentire alle autorità di gestione di svolgere i compiti relativi al monitoraggio e alla valutazione in conformità i requisiti di cui all'articolo 56 del CPR e gli articoli 5 e 19 e agli allegati I e II del regolamento del FSE. L'identificatore univoco dell'autore permette di essere rintracciato e ricontattato per chiarimenti sulle operazioni effettuate.

La corretta identificazione dell'autore delle operazioni è correlato alla necessità di distinguere, per dato trattato, tra i casi di mancata risposta (quando i dati sono raccolti direttamente da partecipanti) o non-dati disponibili (quando i dati sono estratti da registri) e le risposte reali.

SIGMA$_{Giovani}$ utilizza internamente dei formati dei campi che ne indentificano lo stato e che consentono di distinguere l'assenza di informazione perché non rilevata, dall'assenza di informazione ma rilevata.

SIGMA$_{Giovani}$ per la trasmissione dei dati si avvale di un'interfaccia web che utilizza il protocollo HTTPS , garantendo intrinsecamente la sicurezza della trasmissione dati.

4. Sicurezza degli accessi

L'accesso al sistema da parte dell'utente avviene mediante l'inserimento di un codice utenza e di una password.

Per richiedere le credenziali di accesso a SIGMAGiovani l'utente può utilizzare una maschera di "Richiesta creazione utenza".

Una volta inserita la richiesta da parte dell'utente, il sistema invia in automatico una email all'indirizzo di posta "sigmautenzeanpal@anpal.gov.it" gestita da Divisione 3 di ANPAL che verifica l'ammissibilità e la correttezza della richiesta.

Fatte le dovute verifiche e se la richiesta di credenziali è ritenuta legittima Divisione 3 di ANPAL informa l'amministratore della sicurezza del sistema di procedere alla creazione dell'utenza.

L'utente finale viene infine informato di aver ricevuto le credenziali che richiedono una modifica della password al primo accesso.

L'utente al momento dell'autenticazione acquisisce i privilegi previsti per il profilo di utenza a cui appartiene.

L'utente viene pertanto abilitato ad operazioni di sola lettura e/o di inserimento/modifica/cancellazione per le singole funzioni ed i singoli campi previsti per il profilo di appartenenza.

Il sistema di profilazione viene gestito da un amministratore della sicurezza del sistema il quale provvede ad assegnare il corretto profilo.

I profili e le utenze sono memorizzati nel database mentre le password sono conservate nel LDAP dell'infrastruttura informatica.

Le password (anche in visualizzazione) sono sempre oscurate e criptate.

La componente di gestione della sicurezza di SIGMA$_{Giovani}$ ™(l'access manager), dispone di un meccanismo parametrico di gestione delle password, della loro scadenza (attualmente impostata a 3 mesi) e del livello di complessità che devono soddisfare per essere ritenute accettabili.

Una volta che la password di accesso è scaduta, dopo i 3 mesi previsti, l'utente può rinnovare la password in autonomia entro i successivi 3 mesi.

Se l'utente non rinnova la password entro i 3 successivi mesi, ossia entro 6 mesi dalla precedente modifica password, l'utenza viene disattivata e non si può più procedere al rinnovo della password in autonomia.

L'utente dovrà dunque richiedere l'assistenza all'amministratore della sicurezza.

Prima di ripristinare una utenza o rinnovare una password, l'amministratore della sicurezza deve essere autorizzato da Divisione 3 di ANPAL (tramite casella di posta "sigmautenzeanpal@anpal.gov.it")

Il sistema dispone di un meccanismo di scadenza della sessione (parametrico) che prevede attualmente il logout dopo 20 minuti di inattività da parte dell'utente.

SIGMA$_{\text{Giovani}}$ prevede l'utilizzo di un set minimale di variabili di sessione, ovvero informazioni che vengono condivise tra una sessione e l'altra, essenzialmente connesse allo stato della navigazione ed alla profilazione. E' invece categoricamente escluso il passaggio delle password tra le sessioni.