Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI
Ufficio federale per l'uguaglianza fra donna e uomo (UFU)

Dichiarazione di sicurezza

Strumento di analisi standardizzato (Logib)
Dimostrazione della sicurezza

1 Contesto

Ai sensi dell'art. 13c cpv. 2 della legge sulla parità dei sessi (LPar), la Confederazione mette a disposizione dei datori di lavoro uno strumento di analisi standardizzato gratuito per l'esecuzione delle analisi della parità salariale. I datori di lavoro che effettuano analisi della parità salariale ai sensi dell'art. 13a LPar con questo strumento di analisi standardizzato possono dimostrare con la presente dichiarazione di conformità la scientificità e la conformità al diritto del metodo ai sensi dell'art. 13c cpv. 1 LPar (v. art. 7 cpv. 3 dell'ordinanza concernente la verifica dell'analisi della parità salariale). Lo strumento di analisi standardizzato (Logib) è stato sviluppato dall'Ufficio federale per l'uguaglianza fra donna e uomo (UFU) all'inizio degli anni 2000 con il sostegno di istituzioni private specializzate. Dal 2020, Logib viene gestito come applicazione web dall'Ufficio federale dell'informatica e della telecomunicazione (UFIT) e dall'UFU.

1.1 Dimostrazione della sicurezza

L'analisi del bisogno di protezione e la protezione di base delle TIC sono state elaborate e messe in vigore in base ai requisiti di sicurezza (protezione di base delle TIC). Nell'allegato è fornita una descrizione chiara e completa dei provvedimenti atti a garantire la sicurezza.

Con la presente, l'Ufficio federale per l'uguaglianza tra donna e uomo (UFU) conferma che lo strumento di analisi standardizzato (Logib) soddisfa tutti i requisiti di sicurezza della Confederazione in conformità con l'analisi del bisogno di protezione e la protezione di base delle TIC. Tramite l'applicazione web non vengono trattati dati particolarmente suscettibili di protezione. L'applicazione web viene sottoposta regolarmente a manutenzione e controlli per accertare la presenza di eventuali lacune in termini di sicurezza.

Berna, ottobre 2020

Aeberhard Patric PURVAM
Digital unterschrieben von Aeberhard Patric PURVAM
Datum: 2020.10.20 08:14:17 +02'00'

Sylvie Durrer	**Markus Grossenbacher**	**Patric Aeberhard**
Direttrice	Responsabile della divisione sicurezza	Esperto di parità salariale
UFU	UFIT	UFU

Allegato alla dichiarazione di sicurezza

Stato	in elaborazione, in verifica, approvato
Versione	2020.2

Indice

Indice delle immagini

Indice delle tabelle

2 Introduzione alla dichiarazione di sicurezza

Il presente documento offre una panoramica delle misure di sicurezza adottate per lo strumento di analisi standardizzato (Logib), che a partire dal capitolo 3.1 sono illustrate nel dettaglio sotto forma di domanda e risposta.

2.1 Cos'è Logib?

Logib [1] è lo strumento di analisi standardizzato della Confederazione per le analisi della parità salariale.

L'Ufficio federale per l'uguaglianza tra donna e uomo (UFU), in collaborazione con l'Ufficio federale dell'informatica e della telecomunicazione (UFIT), ha perfezionato Logib affinché i datori di lavoro possano, da una parte, verificare il rispetto della parità salariale tra donne e uomini attraverso un'autovalutazione e, dall'altra, eseguire controlli negli acquisti pubblici (art. 8 cpv. 1 lett. c LAPub).

2.2 Revisione della legge federale sulla parità dei sessi (LPar), art. 13a segg.

A partire dal 1° luglio 2020 è entrata in vigore la revisione della legge federale sulla parità dei sessi (LPar): pertanto le aziende con un organico pari o superiore alle 100 unità sono tenute a effettuare un'analisi della parità salariale con cadenza quadriennale e a sottoporla al controllo di un organo indipendente. I risultati dell'analisi della parità salariale devono essere comunicati ai lavoratori e agli azionisti. Inoltre, entra in vigore un'ordinanza che disciplina la formazione delle imprese di revisione, la verifica dell'analisi della parità salariale e le scadenze da rispettare [2]. Pertanto, a partire dal 1° luglio, la Confederazione è tenuta a mettere a disposizione dei datori di lavoro uno strumento di analisi standardizzato gratuito ai sensi dell'art. 13c cpv. 2 LPar.

2.3 Dimostrazione della sicurezza

L'analisi del bisogno di protezione [3] e la protezione di base delle TIC [4] sono state elaborate e messe in vigore in base ai requisiti di sicurezza (protezione di base delle TIC).

2.4 Breve descrizione della dichiarazione di sicurezza

Di seguito vengono brevemente elencati i punti salienti della presente dichiarazione di sicurezza:

- i dati restano a disposizione dell'utente solamente nella sessione corrente del browser e pertanto non vengono salvati in modo permanente da nessuna parte;
- i dati possono essere modificati solo in locale nella cache del browser dell'utente. Soggetti terzi non hanno accesso a questi dati;
- alla chiusura del browser, tutti i dati vengono eliminati;
- i dati vengono trasmessi tramite https o in forma crittografata;
- il server di Logib è gestito dall'Ufficio federale dell'informatica e della telecomunicazione.
- L'applicazione Logib si basa su metodi scientifici e conformi al diritto [5].

3 Architettura

In questo capitolo viene fornita una breve descrizione dell'architettura e della sua implementazione tecnica.

3.1 Schema rappresentativo di Logib

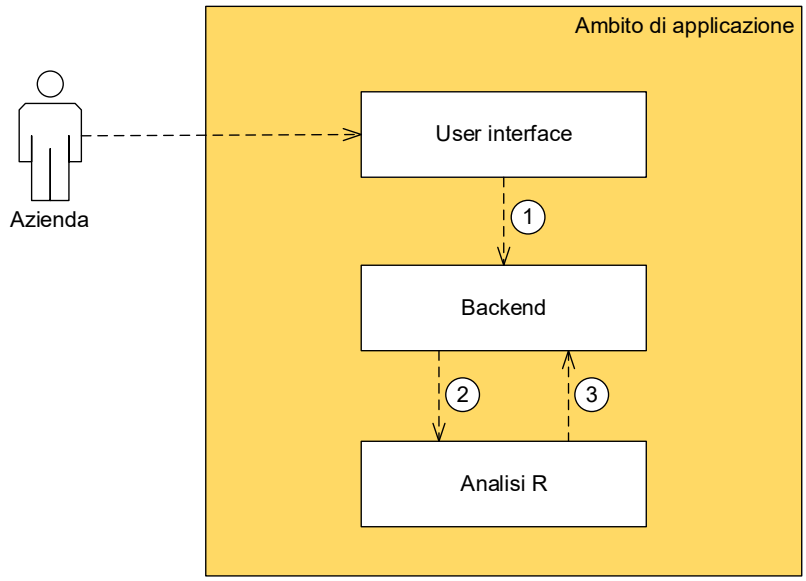


Immagine 1: schema rappresentativo di Logib

3.2 Su cosa si basa Logib dal punto di vista tecnico?

3.2.1 User interface

Questa componente consente di interagire con l'utente.

Nel presente sistema (fase 2), l'utente non deve effettuare il login.

- Controllo di plausibilità dei dati inviati (escl. validazione del numero progressivo)
- Controllo sintattico dei dati inviati
  →https://confluence.bit.admin.ch/pages/viewpage.action?pageId=268097910
- Preparare dal punto di vista grafico i dati della componente di analisi (R) con la libreria software HighCharts di JavaScript

Prodotto/tecnologia

Oblique/Angular sono il framework frontend.

I due moduli «user interface» e «backend» vengono realizzati insieme in un microservizio.

3.2.2 Backend

Nel modulo «backend» si eseguono principalmente le seguenti funzioni:

- caricamento del file di dati e conversione in un file JSON
- trasformazione età, genere, anni di servizio
- validazione del numero progressivo (per motivi di prestazioni non nella UI)
- i dati vengono inviati a R in formato JSON e ricevuti a loro volta nello stesso formato da R

Prodotto/tecnologia

.NET Core 3.x

→Piattaforma software gratuita e open source della piattaforma .NET, utilizzata per lo sviluppo e l'esecuzione di programmi applicativi e sviluppata con il coordinamento di Microsoft.

I due moduli «user interface» e «backend» vengono realizzati insieme in un microservizio e si trovano nello stesso container.

3.2.3 Analisi R

La componente «analisi R», che funge da backend, si occupa esclusivamente dei calcoli (base per: standardizzazione dei salari, analisi di regressione, numeri nel cockpit). Non vengono preparati grafici, tabelle, ecc.

I dati vengono trasmessi dal backend sotto forma di file JSON.

Una volta effettuati i calcoli, i risultati vengono rispediti al backend nello stesso formato di file.

Informazioni particolareggiate sugli attributi sono fornite nella descrizione dettagliata delle interfacce (v. cap. 4.1.2 Flusso di dati).

Prodotto/tecnologia

- Plumber (REST API) per la comunicazione dei moduli «backend» e «analisi R».
- Il modulo «analisi R» viene implementato in un container a parte.

3.3 Dove sono collocati i server?

I server si trovano nei locali del centro di calcolo dell'Ufficio federale dell'informatica e della telecomunicazione in Svizzera.

3.4 Come si può accedere a Logib?

3.4.1 Accesso interno

Gli amministratori di sistema così come gli sviluppatori e i tester dell'applicazione devono necessariamente accedere a questa attraverso un ruolo utente personalizzato.

3.4.2 Accesso esterno

L'applicazione viene usata dagli utenti delle aziende che eseguono un'analisi salariale.

3.5 Visualizzazione della rete

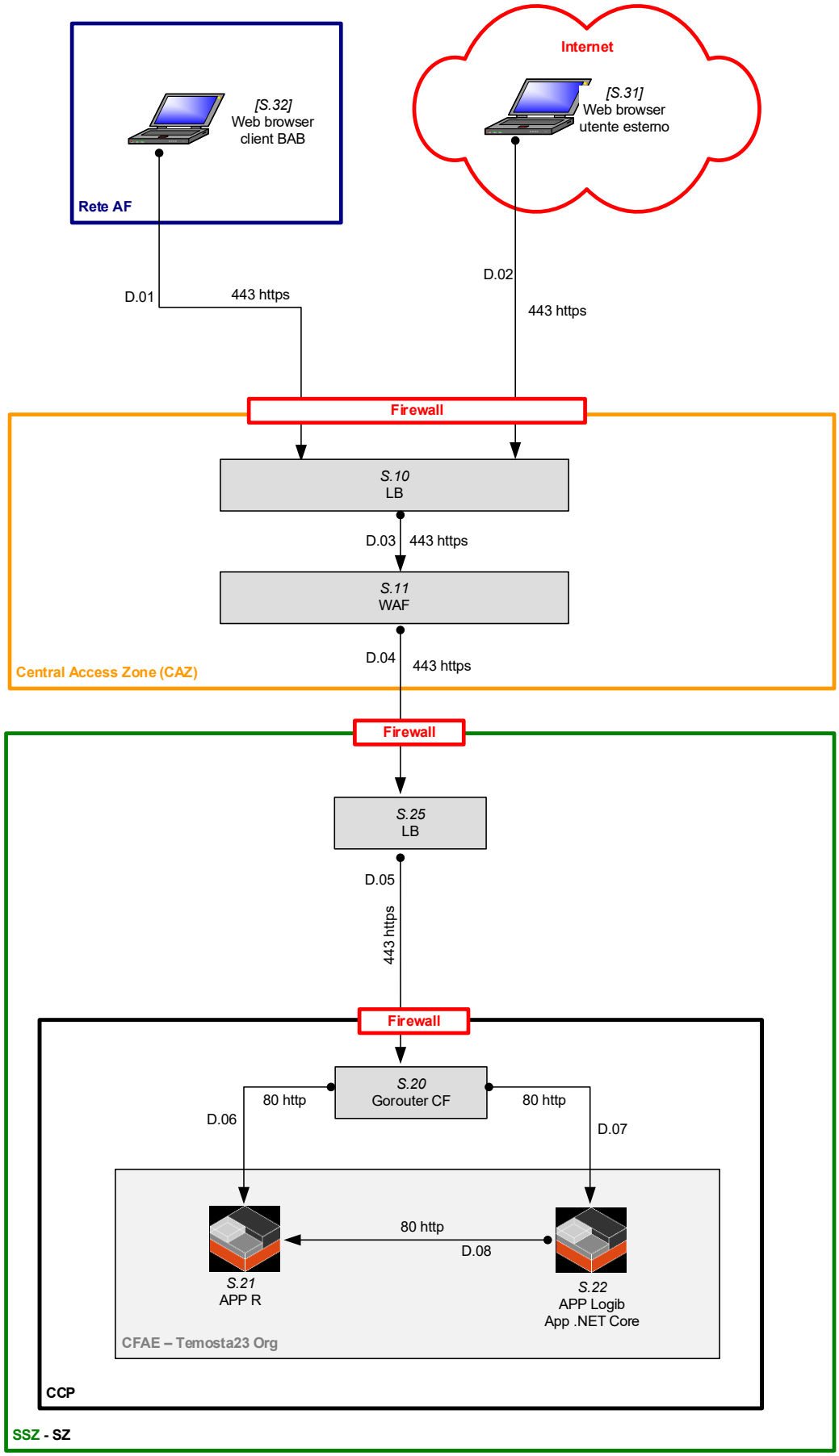


Immagine 2: Visualizzazione della rete

4 Riservatezza

4.1 Dati

4.1.1 Cosa ne è dei dati durante l'esecuzione dell'analisi?

1. I dati vengono letti in locale nel browser dell'utente.
2. Per non sovraccaricare il browser, l'analisi viene eseguita sul server dell'Ufficio federale dell'informatica e della telecomunicazione. A tale scopo vengono trasmesse tramite un collegamento crittografato solo informazioni obbligatoriamente necessarie. Nel corso di questa procedura non vengono salvati dati sul server e non è possibile risalire all'azienda. Questa procedura garantisce inoltre che possano essere elaborati anche corposi file di dati di grandi aziende.
3. L'analisi viene eseguita nello strumento statistico «R» e non in locale nel browser. Il codice del programma per l'esecuzione dell'analisi non è banale di per sé. Per la sua implementazione è più indicato lo strumento «R» rispetto ai linguaggi JavaScript che vengono utilizzati nel browser.
4. Il risultato dell'analisi della parità salariale viene rispedito al browser.

Il flusso di dati può essere schematizzato come mostrato di seguito. Per una rappresentazione più leggibile fare riferimento all'allegato cap. 11:

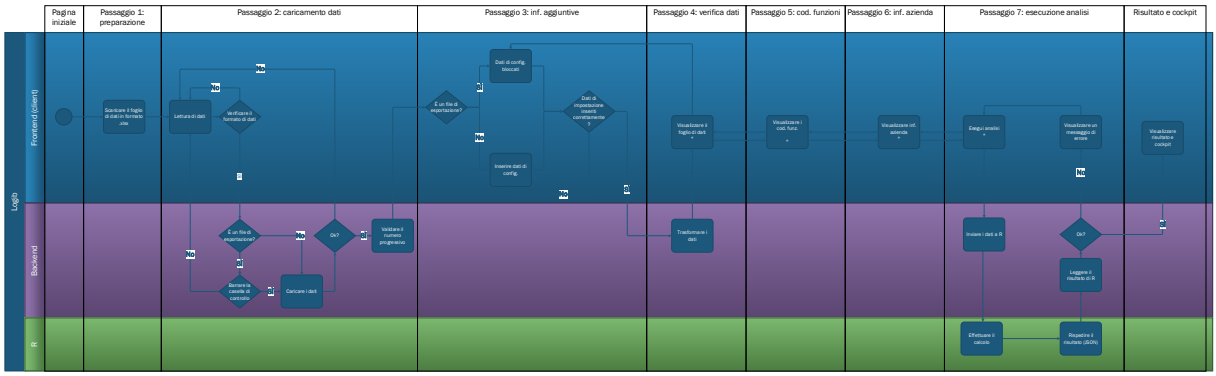


Immagine 3: flusso di dati Logib

4.1.2 Flusso di dati

Spiegazione sul flusso di dati:

Passaggio 1: preparazione e procedura	01 – Scaricare il foglio di dati in formato .xlsx	L'utente può scaricare il foglio di dati in formato Excel.
Passaggio 2: lettura di dati	02 – Lettura di dati	Il foglio di dati compilato dall'azienda viene letto in Logib.
	03 – Verificare il formato di dati	Il formato del foglio di dati viene verificato.
	04 – È un file di esportazione?	Il foglio di dati è un file di esportazione? SÌ / NO

	05 – Barrare la casella di controllo	Se si tratta di un file di esportazione, occorre barrare la casella di controllo.
	06 – Lettura di dati	I dati vengono letti nel backend.
	07 – Ok?	La procedura «lettura di dati» è stata eseguita correttamente? SÌ / NO
	08 – Validare il numero progressivo	Il numero progressivo viene validato [→ i dati vengono inviati al backend e si verifica che non vi siano doppioni]
Passaggio 3: informazioni aggiuntive	09 – È un file di esportazione?	Il foglio di dati è un file di esportazione? SÌ / NO
	10 – Dati di config. bloccati	Nel passaggio 3 non si possono inserire dati di configurazione.
	11 – Inserire dati di config.	I dati di configurazione devono essere inseriti.
	12 – Dati di impostazione inseriti correttamente?	I dati di impostazione o di configurazione sono stati inseriti correttamente? SÌ / NO
Passaggio 4: verifica foglio di dati	13 – Trasformare i dati	I dati del foglio di dati vengono trasformati.
	14 – Visualizzare il foglio di dati	Il foglio di dati viene visualizzato.
Passaggio 5: confermare i codici funzione	15 – Visualizzare i cod. funz.	I codici funzione vengono visualizzati (le funzioni vengono riprese da 'Verifica dati').
Passaggio 6: informazioni sull'azienda	16 – Visualizzare inf. azienda	È possibile inserire informazioni sull'azienda (facoltativo).
Passaggio 7: esegui analisi	17 – Eseguire l'analisi	L'analisi viene eseguita.
	18 – Inviare i dati a R	Solo i dati necessari vengono inviati a R.
	19 – Effettuare il calcolo	Il calcolo viene effettuato in R.
	20 – Rispedire il risultato (JSON)	Il risultato viene rispedito al server.
	21 – Leggere il risultato di R	Il risultato viene letto dal server.
	22 – OK?	Il risultato è OK? SI/NO

	23 – Visualizzare un messaggio di errore	Se il risultato non è corretto, si visualizza un messaggio di errore.
Risultato e cockpit	24 – Visualizzare risultato e cockpit[1]	Se il risultato è corretto, l'utente può visualizzare il risultato dell'analisi e il cockpit.

Tabella 1: spiegazione del flusso di dati Logib

Nota: tutti i passaggi contrassegnati con un «*» (ovvero i n. 14, 15, 16, 17) possono essere visualizzati in modalità «read only» dopo che l'analisi è stata eseguita.

4.1.3 I dati vengono salvati?

Nessun dato viene salvato in modo permanente. Si veda anche il punto 4.3.

4.1.4 I dati vengono sottoposti a ulteriori trattamenti?

I dati non vengono sottoposti a ulteriori trattamenti da parte di terzi.

4.1.5 Come si garantisce la sicurezza dei dati?

La sicurezza dei dati si basa su tre elementi fondamentali:

1. Collegamento sicuro

   I dati vengono trasmessi attraverso un collegamento crittografato secondo lo standard TLS.

   TLS (Transport Layer Security) è un protocollo di crittografia atto a garantire una trasmissione sicura dei dati sul web.

2. Dati anonimi (non vengono trasmessi cognomi, nomi, denominazioni relative a funzioni)

   I dati trasmessi sono anonimi e pertanto non sensibili in termini di contenuto.

   La condizione necessaria per garantire ciò è una corretta preparazione dei dati caricati dall'utente. Se nel record di dati vengono inclusi erroneamente cognomi e nomi, saranno trattati anche dati personalizzati. Pertanto è necessario prestare attenzione all'anonimizzazione dei dati in base alle istruzioni.

   L'applicazione Logib non può incidere in alcun modo sulla creazione dei dati forniti dagli utenti.

3. Nessun salvataggio di dati

   I dati non vengono salvati e restano a disposizione solamente durante la sessione corrente.

4.1.6 I dati sono visualizzabili?

I dati possono essere visualizzati solo dall'utente. I documenti generati non vengono salvati da nessuna parte né trasmessi a terzi. Possono essere scaricati durante la sessione corrente dall'utente o dagli utenti.

[1] I template vengono inviati dal frontend al backend, dove vengono compilati con i relativi dati → openxml inserisce le variabili dei template.

4.2 Trasmissione dei dati

4.2.1 Crittografia

I dati sono trasmessi in forma crittografata secondo lo standard TLS tramite https.

4.3 Eliminazione dei dati

4.3.1 Come vengono eliminati i dati?

Alla chiusura del web browser, anche i dati caricati vengono eliminati. Pertanto non è possibile chiudere il browser temporaneamente e poi accedere nuovamente ai dati caricati in precedenza e alla loro valutazione. In qualsiasi momento, l'utente può salvare in locale i dati salvati nella cache del browser usando la funzione «Esportazione del foglio di dati in formato Excel» per poterli importare nuovamente in Logib in un secondo momento e proseguire con l'analisi.

4.4 Dati personali

4.4.1 Quali dati personali vengono caricati nell'applicazione web?

Tutti i collaboratori possono leggere un file, ovvero il foglio di dati sotto forma di modello Excel, nella cache locale del browser. Per l'analisi servono obbligatoriamente i seguenti dati: mese e anno di riferimento, numero progressivo, età, genere, anni di servizio, formazione, funzione, livello di competenza operativa, posizione professionale, grado di occupazione oppure ore retribuite così come i singoli componenti salariali. È possibile inserire anche altri dati di singole persone, come nome, numero AVS e indirizzo, sebbene ciò non sia consigliabile per garantire la riservatezza.

Per l'analisi vengono trasmessi al server R solo i dati necessari (cfr. punto 4.1.1):

- il numero progressivo viene anonimizzato;
- la funzione non è necessaria per l'analisi ed è salvata esclusivamente nella cache locale del browser.

Durante l'analisi, i dati personali rimangono a disposizione nel browser aperto, ma non appena questo viene chiuso, i dati caricati vengono eliminati.

Nel passaggio «Informazioni sull'azienda» della procedura guidata, si possono inserire facoltativamente dati sull'azienda, come la ragione sociale, l'indirizzo, la persona di contatto, il telefono e l'e-mail. Queste informazioni, se utilizzate, vengono trasmesse anche al backend e inserite nei documenti relativi al risultato e nei file di esportazione (p.es. Excel)[2].

4.4.2 Cosa ne è dei dati personali?

I dati personali vengono inviati al backend per il calcolo della parità salariale, e lì vengono conservati nella memory per tutto il tempo in cui vengono usati per l'analisi in corso. I dati, attualmente, non vengono resi persistenti. Si veda la spiegazione dettagliata al punto 4.1.1.

[2] I template vengono inviati dal frontend al backend, dove vengono compilati con i relativi dati, → openxml inserisce le variabili dei template.

4.5 Informazioni classificate

4.5.1 Vengono trattate informazioni classificate ai sensi dell'OPrI?

L'analisi del bisogno di protezione TEMOSTA23 V.1.1 non prevede che il sistema salvi, tratti o valuti dati/informazioni classificati ai sensi dell'OPrI.

4.5.2 Nell'applicazione web vengono trattate informazioni che, ai sensi di una specifica legislazione, richiedono una particolare protezione?

L'analisi del bisogno di protezione TEMOSTA23 V.1.1 non prevede che il sistema salvi, tratti o valuti dati particolarmente suscettibili di protezione.

5 Disponibilità dell'applicazione

5.1 Durata di inattività

5.1.1 Qual è la durata massima di inattività consentita?

La durata di inattività può essere al massimo di 12 ore in base all'elenco dei servizi: classe di disponibilità 1.

5.2 Orari di servizio

5.2.1 Quali sono gli orari di servizio?

Gli orari di servizio sono da lunedì a venerdì, dalle ore 7.00 alle 18.00.

5.3 IT Service Continuity Management (ITSCM)

5.3.1 L'ITSCM è rilevante come parte del Business Continuity Management (BCM) per i processi aziendali critici?

L'ITSCM non è rilevante come parte del BCM. In caso di emergenza, l'intero sito web non viene più messo a disposizione in via provvisoria. Per questo caso vengono sviluppate misure organizzative, come la messa a disposizione di Logib a breve termine con una tecnologia diversa, mantenendo gli stessi standard di sicurezza.

6 Integrità

6.1 Devono poter essere dimostrate l'autenticità, la correttezza e l'integrità dei dati?

L'analisi del bisogno di protezione non prevede nessun particolare requisito in relazione all'integrità.
Poiché l'applicazione viene utilizzata online e il risultato dell'analisi viene fornito solo a chi ha trasmesso i dati, non è necessario implementare una funzione che individui eventuali manipolazioni dei dati durante i vari passaggi.

7 Tracciabilità

7.1 Devono poter essere dimostrati determinati processi lavorativi?

L'analisi del bisogno di protezione della Confederazione non prevede nessun particolare requisito in relazione alla tracciabilità.
Nel capitolo 9 si spiega quali dati vengono salvati nei logfile e dove vengono conservati questi ultimi.

8 Rilevanza per il processo di verifica RINA

8.1 Logib rischia di essere pesantemente compromesso dallo spionaggio dei servizi d'informazione?

Dall'indagine condotta nell'ambito dell'analisi del bisogno di protezione risulta che Logib non è rilevante per il processo di verifica RINA e non sussiste alcun rischio di spionaggio dei servizi d'informazione.

9 Logfile

9.1 Cos'è un logfile?

Nel sistema IT vengono creati logfile standardizzati come base per lo svolgimento dei compiti operativi. L'esercizio del sistema IT è garantito dall'UFIT per quanto riguarda gli aspetti tecnici, mentre la sfera organizzativa e gli spazi sono di competenza dell'UFU. I logfile sono pertanto soggetti alle convenzioni di sicurezza dell'UFIT.
Logib non genera propriamente dei logfile. I container della Cloud Foundry si collegano alla console corrispondente. Questi log vengono resi persistenti dalla piattaforma container per un certo lasso di tempo e possono essere consultati dal team di sviluppatori.

9.2 A quale scopo vengono usati i logfile?

La piattaforma Cloud Foundry, come base tecnica, svolge varie funzioni di protezione contro i cyber attacchi rivolti all'infrastruttura della Confederazione. A tale scopo, tra l'altro, vengono registrati gli indirizzi IP degli utenti. Per ragioni di sicurezza, l'UFIT non comunica questi dati ad altri team. Allo stesso modo, queste informazioni non vengono messe a disposizione neppure di Logib ovvero del team che garantisce l'esercizio IT di Logib e perfeziona lo strumento.

I log generati per l'applicazione Logib vengono usati per analizzare eventuali errori segnalati dagli utenti. Nei log vengono messi in relazione solo i dettagli tecnici dell'errore rilevato, che vengono poi trasmessi con un request ID. In questo modo è possibile individuare in quale punto di un processo sono comparsi più errori di vario tipo. Non è possibile risalire all'utente. A tale scopo vengono registrati temporaneamente i seguenti dati per ogni sessione del frontend, Logib: data, orario, inizio della prima analisi nella procedura guidata e informazioni sugli errori/sui warning. I dati degli utenti non vengono salvati nei log.

Inoltre, separatamente dal frontend, la piattaforma Cloud Foundry riconosce, come già spiegato, l'indirizzo IP.

9.3 Dove vengono salvati i logfile?

I logfile vengono salvati nella piattaforma Cloud Foundry, della cui manutenzione si occupa il team CCP dell'UFIT. Il team CCP appartiene, dal punto di vista organizzativo, a un altro settore.

9.4 Come vengono eliminati i logfile?

I log presenti nella piattaforma Cloud Foundry vengono conservati per 90 giorni per motivi di sicurezza. Dopodiché vengono eliminati automaticamente dalla piattaforma stessa. Questa impostazione può essere configurata nella piattaforma.

9.5 Come viene garantita la sicurezza dei dati contenuti nei logfile?

La piattaforma Cloud Foundry viene messa a disposizione e gestita dall'UFIT. Responsabile della sicurezza dei log, pertanto, è il team CCP dell'UFIT. Gli accessi sono regolamentati in base al piano di sicurezza [SIPD] e accessi per il team CCP.

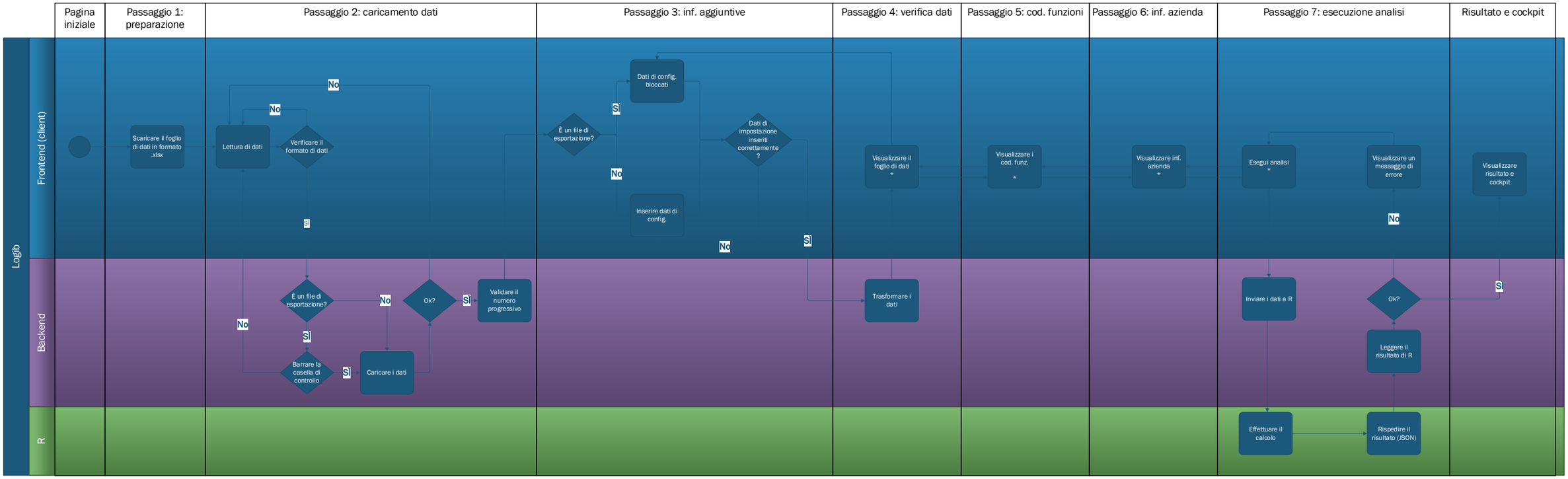
10 Errore di analisi

Se durante l'utilizzo di Logib si verifica un errore, l'utente visualizza un messaggio di errore sotto forma di oblique notification, e i dettagli tecnici dell'errore vengono esportati in un log come descritto nel capitolo 9.

11 Allegato

11.1 Grafico sul flusso di dati Logib

Di seguito è riportato il grafico raffigurante il flusso di dati in Logib:



Nota:

* dopo l'esecuzione dell'analisi, l'utente può visualizzare in modalità «read only» le procedure guidate contrassegnate.

Immagine 4: flusso di dati Logib [ingrandito]

12 Glossario

Termine / abbreviazione	Significato
.NET Core 3.x	Piattaforma software gratuita e open source della piattaforma .NET, utilizzata per lo sviluppo e l'esecuzione di programmi applicativi e sviluppata con il coordinamento di Microsoft.
BCM	Business Continuity Management
Appalti pubblici	Ai sensi dell'art. 8 cpv. 1 lett. c LAPub [6]
UFIT	Ufficio federale dell'informatica e della telecomunicazione [7]
Rete AF	Rete dell'Amministrazione federale
CAZ	Central Access Zone ovvero la zona di accesso centrale
Cloud Foundry	La piattaforma strategica Cloud Foundry e Kubernetes dell'UFIT.
Container	I container sono uno degli attuali trend nel mondo informatico. Accorpano un'applicazione e tutti i file necessari per eseguirla in un pratico pacchetto.
UFU	Ufficio federale per l'uguaglianza fra donna e uomo [8]
LPar	Legge sulla parità dei sessi
HTTPS	L'Hypertext Transfer Protocol Secure è un protocollo di comunicazione del World Wide Web che consiste in una crittografia di trasporto, ovvero consente di trasmettere dati al sicuro da intercettazioni.
OPrI	Ordinanza sulla protezione delle informazioni della Confederazione [9]
ITSCM	IT Service Continuity Management
JavaScript	JavaScript è un linguaggio script originariamente sviluppato per l'HTML dinamico nei web browser.
JSON	JavaScript Object Notation (JSON) è un formato di file compatto in un formato di testo facilmente leggibile, e serve allo scambio di dati tra applicazioni.

Termine / abbreviazione	Significato
LB	Il load balancer serve a ripartire il carico all'interno dell'infrastruttura di un server.
Logfile	Un logfile contiene i registri gestiti automaticamente di tutte o di alcune azioni di processi in un sistema informatico.
Logib	Strumento di analisi standardizzato della Confederazione per le analisi della parità salariale.
Matomo	Programma di analisi gratuito.
Oblique/Angular	Un framework frontend per marchi di UI svizzeri.
Plumber (REST API)	Plumber consente di creare l'interfaccia di un'applicazione web (API) che assicura la comunicazione tra backend e R.
R	Programma (linguaggio di programmazione) open source per calcoli statistici e grafici.
RINA	RINA (metodo di gestione dei rischi impiegato dall'ODIC per ridurre lo spionaggio dei servizi d'informazione) è un processo di verifica.
Schuban	Analisi del bisogno di protezione [3]
SSZ	Shared Service Zone
SZ	Server Zone
TLS	Transport Layer Security, noto anche come Secure Sockets Layer (SSL), è un protocollo di crittografia ibrido atto a garantire una trasmissione sicura dei dati sul web.
UI	User interface (UI) è l'equivalente inglese di interfaccia utente, che sta a indicare i modi in cui un utente entra in contatto con una macchina.
WAF	Il Web Application Firewall (WAF) è una procedura atta a proteggere le applicazioni web da attacchi attraverso l'HTTP.

Tabella 2: Glossario

13 Bibliografia

[1] Ufficio federale per l'uguaglianza fra donna e uomo (UFU), «Analizzare la parità salariale in modo semplice e sicuro con Logib» [Online]. Available: www.logib.ch. [Consultato il giorno 26 06 2020].

[2] Ufficio federale per l'uguaglianza fra donna e uomo (UFU), «Domande e risposte sull'analisi della parità salariale secondo la legge federale sulla parità dei sessi (LPar)» [Online]. Available: https://www.ebg.admin.ch/ebg/de/home/themen/arbeit/lohngleichheit/lohngleichheitsanalyse-gleichstellungsgesetz.html#2035398151. [Consultato il giorno 26 06 2020].

[3] <Organo direzione informatica della Confederazione (ODIC), «PO41 - Analisi del bisogno di protezione (Schuban),» 28 01 2020. [Online]. Available: https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/prozesse-methoden/p041-schutzbedarfsanalyse_schuban.html. [Consultato il giorno 26 06 2020].

[4] Organo direzione informatica della Confederazione (ODIC), «Si001 - Protezione di base delle TIC nell'Amministrazione federale» 22 12 2019. [Online]. Available: https://www.isb.admin.ch/isb/de/home/ikt-vorgaben/sicherheit/si001-ikt-grundschutz_in_der_bundesverwaltung.html. [Consultato il giorno 26 06 2020].

[5] Ufficio federale per l'uguaglianza fra donna e uomo (UFU), « Dichiarazione di conformità Logib,» 18 03 2020. [Online]. Available: https://www.ebg.admin.ch/dam/ebg/de/dokumente/lohngleichheit/logib/konformitaetserklaerung_logib.pdf.download.pdf/Konformit%C3%A4tserkl%C3%A4rung_Standard-Analyse-Tool%20(Logib)_V2020.1.pdf. [Consultato il giorno 26 06 2020].

[6] Il Consiglio federale, «172.056.1 - Legge federale sugli acquisti pubblici» 20 06 2020. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/19940432/index.html. [Consultato il giorno 26 06 2020].

[7] Ufficio federale dell'informatica e della telecomunicazione (UFIT), «Home» [Online]. Available: https://www.bit.admin.ch/bit/de/home.html. [Consultato il giorno 26 06 2020].

[8] Ufficio federale per l'uguaglianza fra donna e uomo (UFU), «Home» [Online]. Available: https://www.ebg.admin.ch/ebg/de/home.html. [Consultato il giorno 26 06 2020].

[9] Il Consiglio federale, «Ordinanza sulla protezione delle informazioni della Confederazione» 01 01 2018. [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/20070574/index.html. [Consultato il giorno 03 07 2020].