Verifica della sicurezza e della disponibilità del sistema GEVER

Cancelleria federale e centro dei servizi informatici del Dipartimento federale dell'economia, della formazione e della ricerca

L'essenziale in breve

Con il programma GENOVA, la Cancelleria federale (CaF) vuole introdurre un unico prodotto per la gestione elettronica degli affari (GEVER) destinato a tutte le unità dell'Amministrazione federale. Pianificato tra novembre del 2015 e settembre del 2021, il programma ha un valore di oltre 68 milioni di franchi. Il centro dei servizi informatici del Dipartimento federale dell'economia, della formazione e della ricerca (ISCeco) è il principale responsabile del funzionamento della piattaforma. Nell'autunno del 2020, già più di 22 000 utenti lavorano con il nuovo sistema.

Con la presente revisione, il Controllo federale delle finanze (CDF) valuta se le misure attuate a livello dell'uso del sistema sono adeguate dal punto di vista della sicurezza e della disponibilità. Controlla anche se la transizione dallo stato di progetto a quello operativo è regolamentata e se le questioni in sospeso vengono monitorate. Infine, questa verifica effettua il monitoraggio di quattro raccomandazioni formulate in occasione di revisioni precedenti.

Il CDF è giunto a una conclusione soddisfacente a livello globale, anche se la complessa architettura del sistema impone esigenze elevate alla gestione e una parte importante del lavoro rimane ancora inconclusa.

I requisiti per la sicurezza sono definiti, ma il processo non è ancora stato completato

L'architettura della soluzione è complessa, diversi attori sono coinvolti nella sua gestione. Le loro prerogative sono definite in maniera chiara ed essi giudicano la collaborazione soddisfacente. Le cariche specialistiche sono ricoperte, il sistema può essere considerato stabile, l'evoluzione degli incidenti è favorevole. Le linee guida, i processi di pianificazione e di gestione sono definiti all'interno dell'ISCeco. Un controllo interno del funzionamento del sistema è stato effettuato e altri sono previsti. Per il CDF, le definizioni dell'organizzazione, delle linee guida e dei processi di gestione sono appropriate. I requisiti per la sicurezza, per quanto riguarda la soluzione tecnica e la gestione, sono documentati. I rischi residui sono riconosciuti e accettati. Tuttavia, il CDF ha constatato che l'attuazione della protezione di base non è pienamente documentata.

Per quanto riguarda i beneficiari delle prestazioni, il CDF non ha esaminato in dettaglio lo stato delle procedure di sicurezza. Ciononostante, ha trovato un caso in cui la ripartizione delle mansioni tra il dipartimento e gli uffici non era stabilita in modo chiaro. Il CDF chiede, in questo caso, un nuovo sforzo di comunicazione.

Protezione dell'accesso e dell'integrità: meccanismi appropriati e alcune questioni da finalizzare

La piattaforma GEVER è installata nel cloud privato («private cloud») dell'Amministrazione federale, ospitata dall'Ufficio federale dell'informatica e della telecomunicazione (UFIT).

Essa viene utilizzata all'interno della rete informatica protetta della Confederazione. L'autenticazione a due fattori è fornita dal servizio TIC standard eIAM[1]. Agli utenti viene assegnato il sistema del loro dipartimento e con esso le autorizzazioni che limitano le operazioni e gli oggetti a cui possono accedere. Viene definito un numero limitato di amministratori, sia a livello di applicazione che tecnico. I meccanismi in atto sono appropriati a livello globale. Tuttavia, il CDF ha constatato che i controlli annuali delle liste di utenti privilegiati non erano ancora operativi.

Una soluzione dell'Aggruppamento Difesa assicura la riservatezza dei documenti fino al livello CONFIDENZIALE. Il regolamento d'uso vieta però il trattamento di documenti di livello SEGRETO e il sistema blocca la definizione di un documento classificato in questa categoria. Il rischio di inserire dati sensibili nei metadati rimane ed è noto al committente.

Il processo di gestione dei cambiamenti in atto presso l'ISCeco definisce adeguatamente le fasi da seguire (richiesta, convalida, esecuzione, test). D'altra parte, i cambiamenti non sono sistematicamente registrati in tutti i componenti del sistema. Il CDF non è stato quindi in grado di controllare l'efficacia del processo di gestione dei cambiamenti. Sono predisposti strumenti che controllano regolarmente l'integrità dei server. Alcune funzioni hash[2] sono disponibili nella piattaforma, ma non ancora in uso. Il CDF ha chiesto dei chiarimenti su questo punto.

Gestione della continuità: il processo non è ancora stato completato

Per soddisfare le crescenti richieste di disponibilità del sistema, l'infrastruttura è progettata in modo ridondante in centri di calcolo separati. I test hanno dimostrato che i dispositivi di memoria funzionano in caso di guasto. Un sistema di monitoraggio dei componenti della piattaforma è attivo presso l'ISCeco, in caso di un grave malfunzionamento vengono emessi avvisi e vengono generate automaticamente richieste di risoluzione dell'incidente. Queste sono poi trattate secondo le procedure in vigore. Il CDF sottolinea che ci sono componenti che non sono sotto il controllo dell'ISCeco. In questi casi, l'ISCeco deve appoggiarsi ad altri fornitori di servizi per la risoluzione degli incidenti.

In termini di gestione del recupero, il CDF constata che ci sono aspetti che non sono ancora stati documentati. Anche se sono state definite diverse misure e si effettuano backup regolari e test di ripristino, manca una visione d'insieme strutturata in questo settore («policy»). Devono essere preparati anche scenari per affrontare guasti, piani di recupero attuali e test di ricostruzione più estesi.

Il passaggio all'organizzazione permanente è regolamentato

Varie attività e istanze sono state definite per affrontare la transizione verso lo stato operativo. Dei gruppi di lavoro a livello direttivo, gestionale ed esecutivo si incontrano regolarmente e coinvolgono le varie parti interessate. In questo modo il trasferimento delle conoscenze viene facilitato. Le questioni in sospeso sono gestite a questi livelli. Il CDF ritiene questi meccanismi adeguati, anche se si aspetta qualche incertezza in relazione alla ripresa delle funzioni dell'ODIC da parte della Cancelleria federale a partire dal mese di gennaio del 2021.

Le precedenti raccomandazioni emesse dal CDF sono state ampiamente attuate.

Testo originale in francese

[1] Servizio TIC standard per la gestione dell'identità e dell'accesso, gestito dall'ODIC.
[2] Funzione crittografica usata per la verifica.