Prüfstelle
Organismo di valutazione
Organn de valutazion

Diritti di accesso e di utilizzo nel sistema SAP

Verifica ai sensi della legge provinciale n. 10/1992, articolo 24, comma 1, lettera a), e successive modifiche

Südtiroler Landtag
Consiglio della Provincia autonoma di Bolzano
Cunsëi dla Provinzia autonoma de Bulsan

AUDITOR	Eva Maria Kofler
AUDITOR	Martin Steinmann

PRÜFSTELLE
ORGANISMO DI VALUTAZIONE

39100 Bozen | Freiheitsstraße 66
39100 Bolzano | Corso Libertà, 66

Tel. 0471 402 212 | Fax 0471 260 114
pruefstelle@landtag-bz.org | organismodivalutazione@consiglio-bz.org
www.landtag-bz.org/de/pruefstelle.asp
www.consiglio-bz.org/it/organismo-di-valutazione.asp
PEC: pruefstelle.organismovalutazione@pec.prov-bz.org
Traduzione: Ufficio traduzioni del Consiglio Provinciale

agosto 2020

INDICE

I. Contesto normativo, motivazione e finalità dell'indagine 4

II. Approccio metodologico e ambito dell'analisi 4

III. Stato di fatto 6

3.1. Ambiente SAP 6

3.2. Livello degli utenti 7

3.3. Livello degli amministratori 9

IV. Valutazioni e raccomandazioni 9

I. Contesto normativo, motivazione e finalità dell'indagine

Ai sensi della legge provinciale n. 10/1992, articolo 24, comma 1, lettera a), e successive modifiche, l'Organismo di valutazione monitora il funzionamento del sistema di controllo interno (di seguito SCI) dell'amministrazione provinciale. Lo SCI ha lo scopo di garantire che il raggiungimento degli obiettivi organizzativi non sia compromesso da rischi interni ed esterni.

Le verifiche sullo SCI sono particolarmente utili nei settori in cui esiste un rischio rilevante. La rilevanza del rischio dev'essere misurata, da un lato, sull'entità del potenziale danno monetario e, dall'altro, sulla potenziale limitazione della funzionalità delle prestazioni. Nel settore dell'informatica si manifestano rischi sempre maggiori, riguardo p. es. alla sfera privata nonché alla sicurezza e integrità di dati e informazioni. L'organizzazione dei diritti di accesso e di utilizzo dei sistemi informatici svolge quindi un ruolo centrale nel contenimento e nella prevenzione di tali rischi.

Nel 2015 l'Organismo di valutazione ha effettuato una verifica generale dello SCI, e negli anni successivi verifiche specifiche in settori selezionati. Nell'ambito del programma di lavoro annuale per il 2020 e al fine di diversificare i settori da controllare, l'obiettivo della presente verifica è stato valutare il funzionamento dello SCI riguardo all'utilizzo del sistema SAP nell'amministrazione provinciale. L'indagine si basa sull'attuale sistema dei diritti di accesso e di utilizzo, che dovrebbe coprire i diversi aspetti di uno SCI efficace.

II. Approccio metodologico e ambito dell'analisi

Da anni, accelerare l'informatizzazione è uno dei principali obiettivi dell'amministrazione provinciale altoatesina[1]. Questo sviluppo viene rafforzato dall'esperienza acquisita con la pandemia di Covid-19. Un'amministrazione pubblica informatizzata porta molti benefici, sia per i cittadini e le imprese che per l'amministrazione stessa. Ci sono però anche dei rischi (sfera privata, segreto d'ufficio), che devono essere analizzati e tenuti in considerazione.

In questo ambito hanno un ruolo centrale i sistemi informatici. Secondo l'associazione senza fini di lucro ISACA Deutschland e.V. (Information Systems Audit and Control Association), un sistema informatico è un sistema socio-tecnico che comprende componenti tecniche (hardware, software, dati), organizzative (ruoli, diritti di accesso) e funzionali (processi aziendali), nonché diversi valori di varia complessità che devono essere protetti[2]. Secondo la ISACA, considerata un punto di riferimento mondiale per la IT-governance (amministrazione e sicurezza dei sistemi informatici)[3], gli obiettivi da perseguire sono i seguenti:

- evitare le violazioni di leggi e di altri regolamenti
- proteggere a lungo termine l'azienda dai danni, monetari e non, causati dai sistemi informatici, nonché dai danni ai sistemi stessi
- mantenere efficienti le prestazioni informatiche, e con esse i processi e i modelli aziendali
- garantire il sistema di controllo interno (SCI) nell'ambito dell'informatica.

Quello dell'informazione è un ambito importante, sia per l'amministrazione pubblica che per le organizzazioni del settore privato[4]. Le informazioni possono esistere in diverse forme – memorizzate o trasmesse elettronicamente, scritte, come immagine o in forma orale. Questa descrizione è conforme

[1] Alto Adige digitale 2020: http://www.provincia.bz.it/informaticadigitalizzazione/digitalizzazione/downloads/ALTOADIGE_DIGITALE_2020.pdf
[2] https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_ii_2016_gesamt_screen.pdf
[3] https://www.agendadigitale.eu/infrastrutture/centri-di-elaborazione-dati-ced-cose-come-funziona-costi-e-normativa/
[4] Manuale austriaco sulla sicurezza: https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf

alla definizione di documento amministrativo nell'articolo 24 della legge provinciale 23 ottobre 1993, n. 17, "Disciplina del procedimento amministrativo".
Il fatto che, ormai, sempre più settori della vita quotidiana non possono funzionare senza i sistemi informatici attribuisce importanza crescente al problema della sicurezza delle informazioni e dell'informatica[5].
È quindi una necessità gestire correttamente le grandi quantità d'informazioni archiviate in questi sistemi. Dell'eccezionale importanza di tale ambito per la protezione delle informazioni il legislatore italiano ha tenuto conto, oltre che con disposizioni di diritto penale (articolo 615-ter CP), anche con una serie di norme a tutela della sfera privata. Il garante per la protezione dei dati personali ha emanato disposizioni particolari per gli amministratori di questi sistemi ("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema")[6]. Gli amministratori hanno quindi un ruolo centrale, perché possono avere una visione d'insieme e accedere a tutte le informazioni. Sono dunque essenziali le procedure per il rilascio ordinato e documentato dei diritti di accesso, che regolano le possibilità di utilizzo. Queste procedure dovrebbero applicarsi all'intera durata (life cycle) del diritto di utilizzo, cioè dalla creazione di nuovi conti (account) utente fino alla loro rimozione quando l'accesso non è più necessario. Particolarmente importante è il controllo dei diritti di accesso privilegiato (superutente, superuser), perché potrebbero servire ad annullare i controlli di sistema[7].

Nella presente analisi l'Organismo di valutazione si basa anche sui seguenti aspetti rilevanti per lo SCI:

- **principio di trasparenza e di tracciabilità:** regole chiare, dettagliate e trasparenti che disciplinino i flussi di lavoro; i documenti e le procedure devono essere registrati in modo da essere tracciabili;
- **automatismi di controllo e principio "dei quattro occhi"**: recepimento sistematico di controlli nell'iter operativo; tali controlli possono avvenire con strumenti informatici o verifiche incrociate;
- **principio della separazione delle funzioni:** nessuna responsabilità esclusiva per l'intero processo; coerente separazione delle funzioni decisionale, esecutiva e di controllo;
- **fornitura di informazioni adeguate ai compiti e alle responsabilità** (principio dell'informazione essenziale): fornire a dirigenza e collaboratori le informazioni di cui hanno bisogno per svolgere i loro compiti;
- **adeguata limitazione dei diritti di accesso e di utilizzo dei dati (principio dei "diritti minimi"):** i diritti di accesso e utilizzo (p. es. ai sistemi informatici) devono essere adeguatamente limitati, e i dati sensibili essere consultabili solo da chi ne ha assolutamente bisogno per espletare le proprie funzioni;
- **SCI inteso come processo in costante divenire:** sua revisione regolare e sistematica riguardo a funzionalità, efficacia e attualità a medio e lungo termine nonché per adeguarlo alle mutate condizioni generali;
- **principio della ponderazione costi-benefici**: costi e risorse per i controlli devono essere proporzionati al rischio che s'intende scongiurare (cioè a entità e probabilità del danno).

Per questa indagine è stato elaborato un questionario basato sui succitati aspetti rilevanti per lo SCI. Il questionario è stato presentato alla ripartizione 9 (informatica) in una riunione. Si è concordato d'inviare il questionario alla sola ripartizione 9 che, a sua volta, nell'esercizio della governance ottiene tutte le informazioni eventualmente necessarie tramite la IAA.

Per analizzare le caratteristiche del sistema di controllo interno (SCI) sui diritti di accesso e di utilizzo in ambiente SAP, appare opportuno esaminare dapprima l'ambiente SAP nell'amministrazione provinciale. Uno SCI ben funzionante si basa su regole organizzative. Per questo motivo, nel paragrafo sottostante non si approfondiscono le possibilità tecniche e le soluzioni offerte dalla SAP come standard. Poi, nei due paragrafi successivi, sono analizzati il livello degli utenti e quello degli amministratori.

[5] Manuale austriaco sulla sicurezza: https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf
[6] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499
[7] Manuale austriaco sulla sicurezza: https://www.sicherheitshandbuch.gv.at/downloads/sicherheitshandbuch.pdf

III. Stato di fatto

Come spiegato nel capitolo precedente la presentazione dei fatti è divisa in tre paragrafi, anche per facilità di lettura. L'esposizione si basa sulle risposte scritte e sui documenti forniti dalla ripartizione informatica.

3.1. Ambiente SAP

Nell'amministrazione provinciale altoatesina l'intera gestione finanziaria si svolge da anni con sistemi SAP (Systeme Anwendungen und Produkte in der Datenverarbeitung = Sistemi, applicazioni e prodotti nell'elaborazione dati)[8]. Oltre alla classica contabilità pubblica (kameralistische Buchhaltung), vi rientrano anche la contabilità patrimoniale e la contabilità di bilancio. A breve, anche parti dell'applicativo Human Ressource (HR) saranno utilizzate per la gestione dei dipendenti. I sistemi SAP sono pertanto applicazioni essenziali, in cui vengono elaborate e memorizzate grandi quantità di dati e informazioni. La base per la gestione delle informazioni è la mappatura dell'architettura aziendale dei rispettivi utenti. La ripartizione informatica ci ha comunicato che essa è ancora in preparazione.
Il sistema contabile è utilizzato da 1.037 utenti (tra cui il Consiglio provinciale e l'amministrazione regionale), con 354 ruoli assegnati. Il programma di gestione del personale è utilizzato da 255 utenti, con 75 ruoli assegnati. Nella gestione delle relazioni coi clienti (customer relationship management, CRM) sono definiti quattro diversi ruoli.

La gestione e il monitoraggio degli utenti è una parte importante dello SCI (life cycle management). Secondo le informazioni, negli ultimi sei mesi 212 utenti (più del 20%) non hanno effettuato alcun accesso al sistema contabile. Al momento il controllo annuale degli utenti inattivi non è ancora stato effettuato.

L'Informatica Alto Adige spa (IAA) tiene conto di questa complessità con tre specifici ambiti di attività (service areas)[9]. Trattasi dell'ambito di attività Human Resources Services, in cui vengono gestiti in particolare il sistema Human Capital Management (HCM) e il rilevamento dei tempi lavorati dell'amministrazione provinciale. L'ambito di attività Finance & Accounting Services copre i seguenti elementi fondamentali dell'amministrazione: bilancio finanziario pubblico, civilistico e patrimoniale, gestione finanziaria delle scuole, gestione della tesoreria, ispezione del servizio di riscossione delle imposte e gestione delle liquidazioni. L'ambito di attività Contribution & Payment Services si occupa sia delle domande, sia della gestione e liquidazione di contributi nonché del pagamento d'imposte e multe. Questi tre ambiti di attività sono coordinati da un centro di competenza (CoC) della SAP. Il centro di competenza è composto da esperti del sistema SAP e si occupa di progetti riguardanti tale sistema. Ciascun settore di attività (service area) della IAA è diretto da un service area manager. I service area manager sono i referenti diretti dei demand manager, che sono insediati direttamente presso la ripartizione informatica e costituiscono il collegamento tra la IAA e le diverse ripartizioni. Il ruolo principale dei demand manager è quello d'individuare la domanda di servizi informatici (e delle relative consulenze), i bisogni e le esigenze degli utenti, e di valutare soluzioni innovative ed economiche[10].

In risposta alla domanda su com'è strutturato il sistema di accesso alle varie applicazioni SAP e su quali sistemi operativi queste sono eseguite, si è riscontrato che non c'è uniformità. Per la gestione finanziaria si usa l'AIX (IBM con OS400), e per la programmazione del bilancio col sistema SAP si usa un server

[8] La delibera della Giunta provinciale n. 2852 del 31 luglio 2000 ha autorizzato la gara per la "Nuova amministrazione finanziaria nell'amministrazione provinciale - SIC 07.2000 La delibera della Giunta provinciale n. 2852 del 31 luglio 2000 ha autorizzato la gara per la nuova gestione finanziaria dell'amministrazione provinciale (SIC 07.2000), che è stata aggiudicata all'associazione temporanea IBM/SAP Consulting Italia.", che è stata aggiudicata all'associazione temporanea IBM/SAP Consulting Italia.
[9] https://www.siag.it/it/service-areas
[10] http://www.provincia.bz.it/it/contatti.asp?orga_orgaid=7437

con Windows 2016. La gestione del personale, il modulo CRM e la contabilità di enti e scuole si fanno su Windows NT.

Un gruppo di lavoro composto da analisti di sistema è stato incaricato di creare una panoramica completa dei sistemi SAP, che si trova pertanto in fase di completamento. Alcune applicazioni specifiche del sistema SAP sono già rappresentate in diagrammi. Queste informazioni sull'ambiente SAP sono destinate all'assistenza clienti e a tutti i collaboratori, per fornire una visione d'insieme dei sistemi installati e dei relativi percorsi di comunicazione[11].

Le funzioni di un sistema SAP vengono attivate mediante transazioni che consentono diverse operazioni o attività sui dati (p. es. scrittura, lettura, cancellazione). Le applicazioni avviate utilizzando tali transazioni verificano, al momento dell'attivazione, se l'utente ha i diritti necessari a compiere, sui dati selezionati dall'applicazione, l'operazione richiesta[12]. I diritti vengono concessi assegnando agli utenti dei ruoli. I ruoli indicano quali transazioni possono essere effettuate dal relativo utente. In definitiva è importante che i ruoli descrivano funzioni o posizioni, e non siano attribuiti a singoli collaboratori. D'altra parte, un numero eccessivo di ruoli può risultare disorientante.
I ruoli dell'amministrazione provinciale definiti nel sistema SAP contengono una descrizione essenziale delle relative autorizzazioni. Ad esempio, il ruolo ZPABUFFENT è il ruolo fondamentale dell'ufficio entrate. I ruoli sono definiti attraverso due categorie: la categoria dei ruoli funzionali autorizza a effettuare diverse transazioni, e la categoria dei ruoli organizzativi consente di lavorare per specifici uffici o ripartizioni.
Fondamentalmente, nella gestione dei diritti si tratta di decidere se e come autorizzare certi utenti, o componenti informatiche, ad accedere a certe informazioni o servizi e ad utilizzarli. I diritti di accesso o di utilizzo sono concessi all'utente in base al profilo utente assegnatogli. La gestione dei diritti consiste nello stabilire le procedure necessarie a concedere i diritti, a revocarli e sottoporli a controllo.
La SAP ha concepito i diritti di accesso[13] all'ABAP in modo da proteggere da accessi non autorizzati transazioni, programmi e servizi nei sistemi SAP. In tal modo l'amministratore assegna ai diversi utenti i diritti che definiscono quali azioni il singolo utente può eseguire nel sistema SAP dopo essersi connesso al sistema e aver effettuato l'autenticazione.
In questo contesto l'amministratore utenti ha un ruolo centrale: secondo le dimensioni e il tipo di organizzazione, un singolo amministratore (superutente) o un gruppo di amministratori assume l'incarico di concedere e gestire questi diritti.
Gli utenti accedono alle applicazioni di gestione finanziaria e del personale tramite autenticazione unica (SSO, single sign-on), mentre ciò non avviene ancora per le altre applicazioni. L'accesso SSO ha il vantaggio che tutte le applicazioni vengono avviate con un unico accesso, per cui non è necessario gestire separatamente una password per ogni applicazione. Ne deriva inoltre un minor numero di richieste di nuove password all'help desk, e dunque costi inferiori. L'SSO garantisce una sicurezza ottimale delle informazioni, poiché è possibile determinare in qualsiasi momento chi ha avuto accesso a quali dati e quando. Si riduce così anche il rischio che terzi possano accedere al sistema. Garantire una costante operatività e configurare le varie applicazioni per un unico accesso pone notevoli sfide alle risorse (umane e finanziarie).

3.2. Livello degli utenti

Il diritto è un'autorizzazione a eseguire determinate azioni nel sistema SAP. Esso è quindi essenziale per il corretto utilizzo dell'applicazione. Il sistema dei diritti serve a proteggere dati e informazioni da

[11] https://de.wikipedia.org/wiki/System_Landscape_Directory
[12] https://www.processpartner.ch/wp-content/uploads/2017/03/1.1.5.3_2.-Leitfaden-SAP-Berechtigungen.pdf
[13] Secondo la Wikipedia, l'ABAP è un linguaggio d programmazione proprietario della società SAP, specializzata in programmi. È concepito per programmare applicazioni commerciali in ambiente SAP, e nella struttura di base è vagamente simile al linguaggio di programmazione Cobol.

modifiche o dalla distruzione (sicurezza dei dati) e a impedirne l'uso illecito (protezione dei dati)[14]. Tale quadro non deve però limitare la produttività del sistema.

Nell'amministrazione provinciale sono previsti ruoli universali per le singole ripartizioni, concepiti a misura delle funzioni dei rispettivi titolari. Sono stati istituiti ruoli appositi per le ripartizioni chiave (ripartizione finanze), che coprono una più estesa gamma di ruoli ovvero consentono funzioni trasversali. Così a questa ripartizione è garantito un accesso più ampio, che è necessario allo svolgimento delle sue attività. Per il resto i ruoli sono limitati alla rispettiva ripartizione.

Il processo di gestione degli utenti (life cycle management) è in parte controllato da un flusso di lavoro (workflow) appositamente creato dall'amministrazione provinciale. Il flusso di lavoro messo a disposizione dalla SAP non viene utilizzato. Per le modifiche, la procedura viene avviata dal supervisore competente o dagli utenti autorizzati, con una richiesta di assistenza (ticket) ovvero per posta elettronica. Per le applicazioni concernenti le finanze e il personale, le richieste di modifica sono trasmesse direttamente al centro di competenza della SAP (CoC SAP). Se necessario il centro di competenza inoltra poi le richieste agli amministratori di sistema. Si effettua quindi una verifica delle modifiche richieste. Questo monitoraggio comprende anche un esame della portata e dell'impatto di tali modifiche. Esse non possono normalmente andare oltre la rispettiva area di appartenenza (ufficio), a meno che non si tratti di particolari ripartizioni. Ogni anno si effettua un controllo (audit) sulle licenze utilizzate e sugli utenti.
Avvenuta con successo l'istituzione dei ruoli richiesti, si prende ancora contatto con l'utente per verificare che tutto si sia svolto nel modo migliore.
Questo processo viene eseguito utilizzando il SAP Solution Manager, un'applicazione che permette il funzionamento delle ulteriori applicazioni installate.
Nelle linee guida per l'utilizzo degli strumenti informatici, ai dirigenti è stata segnalata la necessità di notificare i cambiamenti di ruolo o di utenti. Se vengono richiesti ruoli trasversali fra più di una ripartizione, si chiede l'autorizzazione delle ripartizioni interessate.

Fondamentalmente, i ruoli assegnati sono personalizzati per i collaboratori di una ripartizione. Un'eccezione è l'inserimento di clienti e fornitori nel sistema, che può essere effettuato da tutti gli utenti autorizzati. Tuttavia, questi dati possono poi essere modificati solo dall'ufficio entrate e dall'ufficio spese. Quando s'introducono nuovi progetti (transazioni), le necessarie modifiche a ruoli e utenti vengono chiarite e introdotte d'intesa con la rispettiva ripartizione. In ogni caso spetta alla ripartizione decidere. I nuovi ruoli possono essere inseriti solo dal centro di competenza della SAP, dagli amministratori di sistema e dagli assistenti tecnici degli amministratori di sistema.

Riguardo all'attuazione delle direttive generali sulla sicurezza e alla protezione delle password, le modifiche a queste ultime vengono effettuate all'interno del sistema. Allo stesso modo, il sistema blocca l'utente dopo un certo numero di tentativi di accesso (login) non riusciti. Il numero di questi tentativi falliti è attualmente fissato a cinque. Gli utenti possono reimpostare la password in qualsiasi momento, ma non più di una volta al giorno. La nuova password dev'essere diversa dalle cinque utilizzate in precedenza. Gli amministratori di sistema, su specifica disposizione del superiore, possono bloccare l'utente o certe funzioni. Il normale periodo di validità di una password è di 90 giorni. Dove esiste l'accesso SSO, si applicano le regole della cartella attiva (active directory); diversamente dev'essere presentata una richiesta specifica. La cartella attiva permette di concepire una rete secondo la struttura reale dell'azienda o la sua distribuzione spaziale[15]. Si possono così amministrare diversi oggetti (utenti, server, stampanti). Inoltre, un amministratore può organizzare, fornire e monitorare le informazioni concernenti i diversi oggetti.

Un altro aspetto rilevante per la sicurezza riguarda il continuo aggiornamento delle patch ("pezze", "toppe") di sicurezza fornite da SAP e Microsoft, che servono a eliminare eventuali errori, soprattutto

[14] https://de.wikipedia.org/wiki/Berechtigungskonzept
[15] https://de.wikipedia.org/wiki/Active_Directory

lacune nella sicurezza. Della relativa fornitura si occupa la SAP, compatibilmente con la disponibilità di questi prodotti in azienda.

La separazione in diversi gruppi funzionali di utenti viene effettuata assegnando le licenze alle rispettive strutture. A questo fine si possono anche creare gruppi specifici. Attualmente i diversi ruoli sono formati secondo le esigenze degli utenti e assegnati in modo trasversale.

Riguardo invece alla registrazione delle funzioni critiche e a un insieme di regole per separare tali funzioni, è in corso una revisione dei ruoli che prevede – soprattutto per gli amministratori – una separazione tra amministratori di sistema, sviluppatori e sviluppatori esterni. Gli stessi adattamenti sono in corso di realizzazione per gli utenti speciali ovvero di emergenza.

3.3. Livello degli amministratori

Il compito degli amministratori è quello di seguire le reti e i sistemi informatici. A causa dei loro estesi diritti in quanto amministratori, essi rivestono una particolare importanza. La SAP ha istituito una speciale categoria di amministratori: trattasi di superutenti che, indipendentemente dalla loro funzione, hanno accesso all'intero sistema e possono lavorare su di esso. Le regole organizzative in questo ambito sono decisive per realizzare un efficace SCI.

Attualmente, agli amministratori di sistema dell'ambito RUN della IAA sono stati assegnati gli ampi diritti di superutente, per cui possono accedere direttamente al sistema. I dipendenti del centro di competenza della SAP possono creare e assegnare dei ruoli agli utenti. È attualmente in corso una revisione di tali attribuzioni, per arrivare a un'assegnazione più selettiva delle funzioni in questo ambito. Si prevede inoltre d'introdurre un ruolo specifico per l'amministrazione degli utenti e l'autorizzazione dei ruoli.

Solo sviluppatori e amministratori di sistema possono creare e modificare le transazioni. Nessun altro utente è autorizzato a sviluppare e inserire transazioni, nemmeno se conoscesse il relativo codice. Solo gli amministratori di sistema e gli sviluppatori possono attribuire le autorizzazioni all'uso.

L'accesso a transazioni e tabelle classificate come critiche dipende dalle singole transazioni, delle quali sono responsabili solo gli amministratori di sistema. Complessivamente nella SAP è previsto un notevole numero di transazioni. Gli amministratori di sistema e gli sviluppatori hanno accesso a tutte le transazioni. Nel nuovo sistema CRM e S/4 sono previsti tre tipi di ruolo:

- amministratore di sistema: senza limitazioni, a motivo del ruolo stesso
- sviluppatore: incaricato di sviluppare le transazioni, anche transazioni funzionali per il collaudo
- amministratori di funzione: per le transazioni previste solo nell'ambito del ruolo assegnato e coi relativi vincoli organizzativi.

Riguardo ai diritti di accesso e di utilizzo, la ripartizione intende ora gestire le richieste in un modo più strutturato, servendosi del programma Key2help. Inoltre, nei nuovi sistemi saranno previsti ruoli CRM e S/4 per ogni categoria di utenti.

IV. Valutazioni e raccomandazioni

Le applicazioni SAP sono componenti fondamentali del sistema informatico dell'amministrazione provinciale altoatesina e degli enti da essa dipendenti. In tali sistemi è memorizzata una grande quantità di informazioni, che devono essere gestite e protette secondo le disposizioni di legge sulla protezione e la sicurezza dei dati. Tale protezione dev'essere garantita sia verso l'esterno che verso l'interno. Una

gestione dei diritti di accesso e di utilizzo adeguata alle esigenze operative aiuta l'amministrazione ad applicare queste prescrizioni e direttive.

Attualmente le applicazioni SAP funzionano su diversi sistemi operativi, il che rappresenta comprensibilmente una grande sfida per garantire la sicurezza delle informazioni. La standardizzazione dei sistemi rappresenta anche una grande sfida finanziaria, e dipende dalle decisioni strategiche dell'azienda.

Naturalmente le applicazioni SAP offrono diverse possibilità di soluzione, già nella configurazione di base. Queste impostazioni predefinite possono essere configurate individualmente dall'azienda, tenendo conto degli elementi di base del sistema di controllo interno nella gestione dei diritti di accesso e di utilizzo. Al riguardo il livello degli utenti e quello degli amministratori sono regolati in modo diverso. Particolare attenzione è rivolta ai cosiddetti superutenti, che possono avere accesso illimitato al sistema.

Dai documenti pervenuti e dalle informazioni in essi contenute si può constatare, in linea di massima, la consapevolezza dell'importanza del sistema dei diritti di accesso e di utilizzo, ivi compreso un efficace allestimento dello SCI.

Vediamo con favore il fatto che la mappatura dell'intero sistema SAP è in fase di completamento, il che faciliterà la realizzazione dello SCI in tutti gli ambiti. Ciò include anche mettere per iscritto i processi aziendali che ne stanno alla base, coinvolgendo i demand manager.

Generalmente l'accesso ai sistemi si effettua già con l'SSO, e ciò garantisce un ottimo controllo dei diritti di accesso e di utilizzo. L'accesso ai sistemi è stato perfezionato grazie a un'efficace gestione delle password.

Dovrebbero essere intensificati i controlli sugli utenti inattivi e sulle successive disconnessioni dal sistema, anche in termini di tempo. In queste verifiche bisognerebbe coinvolgere maggiormente le ripartizioni. Per un'efficace gestione del ciclo di vita (life cycle management) sarebbe raccomandabile una gestione degli utenti unitaria e basata sulle informazioni, che tenga conto della separazione tra richiesta, rilascio, esecuzione e conferma (workflow).

Per uno SCI ben funzionante nella gestione dei diritti di accesso e di utilizzo, è essenziale trovare un equilibrio tra una dotazione differenziata di ruoli necessari e un eccesso nel numero dei ruoli stessi. Il numero di ruoli attualmente definiti per gli utenti è molto elevato (354). Si raccomanda di verificare attentamente numero e contenuto dei ruoli.

Approviamo la revisione dei profili di ruolo esistenti al livello degli amministratori, compreso l'adeguamento nell'ambito degli utenti speciali ovvero di emergenza. Questo ambito merita, a motivo della sua importanza, un'attenzione particolare.
Mettere per iscritto questi compiti serve a perfezionare ulteriormente uno SCI efficace. Sarebbe inoltre opportuno disporre di una modalità unitaria per creare la banca dati nell'ambito clienti e fornitori, per evitare d'immettere ripetutamente registrazioni (record) di dati anagrafici.

Nel 2021 verrà effettuato un follow-up per valutare l'attuazione delle raccomandazioni.

Vorremmo infine ringraziare la ripartizione informatica per la collaborazione, che è ben riuscita nonostante la particolare sfida posta dalla pandemia di Coronavirus.

18/09/2020

f.to	f.to
Eva Maria Kofler	Martin Steinmann

Südtiroler Landtag
Consiglio della Provincia autonoma di Bolzano
Cunsëi dla Provinzia autonoma de Bulsan

Prüfstelle
39100 Bozen | Freiheitsstraße 66
Organismo di valutazione
39100 Bolzano | Corso Libertà, 66

Tel. 0471 402 212 | Fax 0471 260 114
pruefstelle@landtag-bz.org | organismodivalutazione@consiglio-bz.org
PEC: pruefstelle.organismovalutazione@pec.prov-bz.org
www.landtag-bz.org/de/pruefstelle.asp
www.consiglio-bz.org/it/organismo-di-valutazione.asp