Prüfstelle
Organismo di valutazione
Organn de valutazion

Gestione della sicurezza delle informazioni nell'amministrazione provinciale

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

AUDITOR Martin Steinmann (fino al 9 luglio 2021)
Wolfgang Bauer

Traduzione: Ufficio traduzioni del Consiglio Provinciale

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

settembre 2021

INDICE

I. Motivazione e finalità dell'indagine sulla gestione della sicurezza delle informazioni nell'amministrazione provinciale

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 dei controlli interni (SCI) dell'amministrazione provinciale.
Questo lavoro è documentato nelle relazioni redatte finora[1].

Il programma di lavoro per il 2021 comprende anche un'indagine sulla gestione della sicurezza delle informazioni nell'amministrazione provinciale, dato il significato strategico e trasversale[2] del tema[3],

L'obiettivo dell'indagine è analizzare e valutare il funzionamento dello SCI riguardo alla gestione della sicurezza delle informazioni, esaminando e valutando gli aspetti della protezione di base in ambito informatico.

II. Ambito e approccio metodologico

L'indagine si concentra sul sistema di sicurezza informatica, tenendo conto sia degli aspetti di governance che di quelli operativi. Trattandosi di un'indagine sul sistema e l'organizzazione, gli aspetti puramente tecnici non vengono esaminati in dettaglio.

Ai fini dell'indagine sono state considerate le cinque componenti dello SCI secondo il modello COSO[4]:
-*ambiente di controllo*
-*valutazione dei rischi*
-*attività di controllo*
-*informazione e comunicazione*
-*monitoraggio*

Specialmente nella sicurezza informatica, l'ambiente di controllo e la definizione degli obiettivi di sicurezza, la valutazione dei rischi e l'adozione di misure appropriate sono di fondamentale importanza. Componenti importanti di un modello efficace di SCI sono anche la comunicazione, sia interna che esterna, nonché il costante monitoraggio.

L'indagine si è basata su un questionario dettagliato indirizzato alla ripartizione informatica, che si concentra sui seguenti ambiti: **gestione della sicurezza, organizzazione e personale, infrastruttura,**

[1] Pubblicate sul sito dell'Organismo stesso: https://www.consiglio-bz.org/it/organismo-di-valutazione.asp

[2] Secondo il piano triennale per l'informatica nella pubblica amministrazione 2020-2022, la sicurezza informatica è trasversale a tutta la strategia nazionale per l'innovazione tecnologica e l'informatizzazione (p. 48).

[3] Il tema della sicurezza diventa sempre più importante anche riguardo all'introduzione di modelli di lavoro agile.

[4] COSO: Committee of Sponsoring Organizations of the Treadway Commission. Il modello, riconosciuto a livello mondiale, ha combinato diversi concetti e definizioni di controllo interno in un unico concetto di base.

sistemi informatici, reti, criteri di applicazione.[5]

III. Stato di fatto[6]

Gestione della sicurezza

*Per **gestione della sicurezza delle informazioni**[7] (GSI) s'intende la funzione di pianificazione, direzione e controllo necessaria a realizzare e mantenere costantemente un processo ponderato ed efficace per garantire la sicurezza delle informazioni. In questo gioca un ruolo centrale il responsabile della sicurezza delle informazioni, assicurando che i sistemi informatici dell'organizzazione siano sempre adeguatamente protetti, raggiungendo e mantenendo così il desiderato livello di sicurezza dei dati e delle informazioni.*

In risposta alla domanda se sia stato nominato un **responsabile della sicurezza delle informazioni**, la ripartizione informatica comunica che presso l'Informatica Alto Adige spa (IAA)[8] questa figura è stata formalmente nominata nel 2018 e che per la ripartizione è stata fatta una nomina nel 2001, che però non è stata rinnovata. Su richiesta la ripartizione spiega che, fino alla conclusione del processo di sviluppo organizzativo recentemente avviato (che interesserà anche il ruolo del responsabile della sicurezza delle informazioni) i compiti di pianificazione, coordinamento e monitoraggio della sicurezza delle informazioni saranno svolti dal responsabile della trasformazione digitale[9], assistito dalla collaboratrice designata nel 2001.

Non c'è una **direttiva generale** della Giunta provinciale sulla sicurezza, in forma di documento programmatico a sé stante che regolamenti una struttura organizzativa finalizzata alla sicurezza delle informazioni. La ripartizione comunica che la IAA, riguardo agli obiettivi di sicurezza delle informazioni e alla relativa strategia, aderisce ai principi guida del piano triennale per l'informatica (capitolo 6)[10].

La ripartizione informatica conferma che per attuare questa strategia si applica un **piano di sicurezza** aggiornato, che mappa in modo completo tutti i processi aziendali e le applicazioni e descrive la procedura per raggiungere gli obiettivi. L'inquadramento e la gestione dei rischi si effettuano su questa base, con modalità che vengono costantemente aggiornate.

Riguardo al **piano di gestione dei rischi**, la ripartizione comunica che per mappare come previsto tutte le attività ci si serve di una piattaforma dell'Agenzia per l'Italia digitale (Agid) basata su internet, che viene così a costituire un sistema di gestione dei rischi basato su IRAM2 (*Information Risk Analysis Methodology*) e ISO 31000 (linee guida per la gestione dei rischi).

In caso di violazione di dati (*data breach*) nell'amministrazione provinciale e nella IAA, oltre al **piano**

---

[5] Fonti principali e documentazione di riferimento per la presente indagine: Bundesamt für Sicherheit in der Informationstechnik (BSI, ufficio federale per la sicurezza informatica); Agenzia per l'Italia digitale (Agid); Klaus-Rainer Müller, *IT-Sicherheit mit System*, Springer Vieweg, 2018.

[6] Le definizioni contenute nel testo seguente sono tratte essenzialmente dallo *IT-Grundschutzkompendium* e da vari standard del BSI: https://www.bsi.bund.de/DE/Home/home_node.html

[7] La GSI è un tema centrale della famiglia ISO/IEC 27000.

[8] Sull'esercizio della governance riguardo alla IAA vedi la relazione dell'Organismo di valutazione "Legittimità, imparzialità e buon andamento dell'azione amministrativa", febbraio 2018.

[9] Il responsabile della trasformazione digitale ai sensi del Codice dell'amministrazione digitale (CAD), articolo 17, è stato nominato con delibera della Giunta provinciale n. 85/2018.

[10] https://pianotriennale-ict.italia.it/piano/.. Vedi anche la circolare dell'Agid n. 2/2017 sulle misure minime di sicurezza informatica per la pubblica amministrazione.

di comunicazione di emergenza si applica un'apposita procedura ai sensi del Regolamento generale sulla protezione dei dati. Queste procedure sono state coordinate tra la ripartizione, l'IAA e i responsabili della protezione dei dati. E, secondo la ripartizione, verranno sottoscritte quest'anno (o al più tardi nel 2022, dopo la conclusione del succitato processo di sviluppo organizzativo), come allegato al nuovo accordo quadro tra amministrazione provinciale e IAA.

Per controllare lo **stato della sicurezza delle informazioni** si effettuano regolarmente operazioni, ad esempio test di penetrazione e valutazioni della vulnerabilità (*vulnerability assessment*). Inoltre, oltre all'auditor esterno per la verifica in base alla norma ISO 27001, c'è una funzione di controllo interno; questa è formalmente indipendente ed esegue regolarmente verifiche di sicurezza in conformità alla norma ISO 27001.

La ripartizione conferma che gli **incidenti relativi alla sicurezza** vengono individuati, gestiti in modo controllato, documentati e sottoposti a ulteriore esame (gestione degli incidenti relativi alla sicurezza secondo le norme ISO 9001 e ISO 27001).

Anche il **piano di backup dei dati** e le **prove** regolari **di recupero** si basano sulla norma ISO 27001.

Il **piano di sicurezza** include anche i servizi cloud esterni; ciò è garantito anche dalle prescrizioni dell'Agid per gli acquisti nell'ambito delle tecnologie dell'informazione e della comunicazione.

La **gestione della sicurezza delle informazioni è certificata secondo la norma ISO 27001**. Tale certificazione riguarda esclusivamente la IAA, ed è stata rinnovata solo recentemente (giugno 2021) in seguito a un controllo esterno. Le osservazioni e raccomandazioni formulate in quella sede sono già state recepite ovvero attuate nel quadro di scadenze e interventi specifici.[11]

Organizzazione e personale

*I requisiti generali e trasversali nell'ambito dell'**organizzazione** devono contribuire a elevare il livello di sicurezza delle informazioni. A tal fine è necessario regolamentare i flussi di informazioni, i processi, la suddivisione dei ruoli nonché la struttura organizzativa e operativa.*
***Collaboratori e collaboratrici** hanno l'importante compito di garantire la sicurezza delle informazioni. Devono quindi essere sensibilizzati ai rischi della sicurezza[12] sistematicamente e in modo mirato, e formati specificamente sui temi della sicurezza delle informazioni.*

Assunzioni, cessazioni dal servizio e cambiamenti organizzativi riguardo al personale vengono formalmente comunicati tra la ripartizione personale e il sistema informatico con lo strumento IT Service Management (ITSM) Ky2Help. Anche le credenziali del personale dell'amministrazione provinciale (*provisioning, de-provisioning*) sono comunicate tramite un workflow, disponibile alla dirigenza e agli assistenti informatici interni/alle assistenti informatiche interne. In attesa di una completa automazione, viene revisionato il collegamento tra ripartizione personale e SAP/AS400.

La ripartizione comunica che non si effettuano **controlli di sicurezza sui nuovi/le nuove dipendenti** del settore informatica.

La suddetta **formazione e sensibilizzazione** di tutti i/tutte le dipendenti riguardo alla sicurezza delle informazioni è compresa in un programma di aggiornamento basato sull'apprendimento via internet, su questionari e su attacchi simulati. Alla domanda se i risultati della formazione vengono valutati, la ripartizione risponde che la piattaforma di apprendimento include alcuni strumenti che si utilizzano a

[11] Sull'importanza della certificazione del sistema di GSI vedi BSI-Standard 200-1, cap. 9.

[12] Sulla cultura della sicurezza vedi: "Cybersecurity-Audits – Bedeutung und Messung der Informationssicherheits-Awareness", *ZIR* 1/2021, p. 16 sgg.; Piano triennale per l'informatica nella pubblica amministrazione 2020-2022, p. 46.

formazione completata, per verificare concretamente le reazioni del personale, p. es. a messaggi di phishing. La ripartizione non spiega come venga valutato in generale il livello di consapevolezza dei rischi e della sicurezza tra i/le dirigenti e i/le dipendenti dell'amministrazione provinciale.

Per pianificare e porre in atto le **modifiche all'architettura informatica**[13] si applica una procedura formale nel quadro del sistema ITSM Ky2Help.

La ripartizione conferma che i **contratti nel settore dell'informatica** tengono conto degli aspetti di sicurezza, che vengono documentati e verificati in accurata osservanza delle linee guida dell'Agid per gli acquisti in tale ambito (vedi sopra).

Infrastruttura

*Per **infrastruttura** s'intendono gli edifici, i locali, la fornitura di energia, l'impianto di condizionamento dell'aria e il cablaggio utilizzati per l'elaborazione delle informazioni: sono dunque esclusi i sistemi informatici e gli elementi di accoppiamento di rete come i router.*

Mediante meccanismi di autenticazione e autorizzazione necessari per l'accesso fisico o via rete, la ripartizione informatica garantisce che l'**accesso all'infrastruttura informatica** da parte di persone non autorizzate sia impedito ovvero monitorato.

I **visitatori** sono soggetti a registrazione e non sono autorizzati a muoversi non accompagnati; il **personale esterno** (p. es. di pulizia) deve esibire un distintivo per accedere ai locali.

La ripartizione conferma l'esistenza di un **piano antincendio** per le sale computer, che è conforme alla normativa vigente.

Viene confermata anche l'adeguata **climatizzazione** delle sale server, delle sale per l'infrastruttura tecnica (p. es. sale di distribuzione) e del centro informatico, comprese le segnalazioni automatiche in caso di anomalie. Lo stesso vale per il monitoraggio automatico dei **parametri ambientali** come temperatura e umidità.

All'interno della IAA sono garantite le misure volte a consentire il **proseguimento delle attività informatiche in caso d'interruzione di corrente**: gruppo di continuità (UPS), generatore di emergenza. Viene anche regolarmente verificata l'efficacia di tutte le misure in caso d'interruzione di corrente.

La ripartizione conferma infine che la **documentazione** completa **del cablaggio elettrico e informatico** compreso l'instradamento è presente, ovvero tracciata formalmente, sul sistema ITSM.

Sistemi informatici

*I **sistemi informatici** sono impianti tecnici che consentono di elaborare informazioni e costituiscono un'unità funzionale autonoma. I tipici sistemi informatici sono server, client, telefoni cellulari, smartphone, tablet, componenti per l'"internet delle cose" (Internet of Things), router, switch e firewall.*

[13] Il termine "architettura informatica" comprende vari aspetti della tecnologia dell'informazione (TI) in un'organizzazione: p. es. lo sviluppo di specifiche, modelli e linee guida metodici. Il fine è quello di realizzare una coerente e ben strutturata architettura informatica (Wikipedia, voce in tedesco, settembre 2021).

La ripartizione informatica conferma che tutti i sistemi informatici sono configurati in base al **principio del minimo**: sono cioè rese disponibili solo le funzioni e le informazioni assolutamente necessarie al proseguimento delle attività.

Sistemi operativi e applicazioni vengono regolarmente aggiornati. Inoltre, nell'ambito della gestione delle patch[14], si svolgono controlli/test periodici (almeno una volta l'anno).

Un'apposita regolamentazione per l'uso dei **dispositivi multifunzionali** disciplina la procedura in caso di difetto o restituzione, e garantisce che tali dispositivi abbiano una memoria non volatile dei dati.

Riguardo all'uso di **terminali mobili**, non è garantito (per il momento) che siano adeguatamente criptati; ma si prevede di riconsiderare questo punto.

Le regole per i gateway di sicurezza[15] sono documentate in modo comprensibile, e tutte le attività sono registrate nel sistema ITSM. Anche il corretto funzionamento dei gateway di sicurezza è regolarmente controllato.

Reti

*Un'affidabile **gestione della rete** è un requisito fondamentale per il funzionamento sicuro ed efficiente delle reti moderne. A questo fine la gestione deve integrare tutti i componenti della rete stessa. Si prendono così le misure opportune per proteggere le comunicazioni e le infrastrutture di gestione della rete.*

La ripartizione informa inoltre che ci sono, documentati ufficialmente, **piani di rete** attuali e completi (panoramiche grafiche dei componenti di rete e delle loro connessioni).

La **gestione del sistema e della rete** garantisce il monitoraggio automatico dei sistemi informatici e dei componenti di rete da parte del sistema SolarWinds e la valutazione dei registri eventi.

I componenti della rete sono configurati secondo il **principio del minimo**. La ripartizione comunica che di norma, prima di allestire programmi o sistemi, si verificano l'adeguatezza e la sicurezza delle configurazioni. La **configurazione** dei componenti di rete è **documentata in modo comprensibile**.

Tutti gli **accessi a LAN e WLAN** sono controllati e monitorati; l'accesso da terminali estranei è possibile solo con VPN (*virtual private network*).

Ambiti di applicazione

Riguardo all'**uso di supporti informatici mobili non di ufficio**, la ripartizione informa che in materia esiste un regolamento e che finora, però, non è stata resa operativa alcuna tecnologia per limitare tale uso.

[14] La gestione delle patch consiste nel procurare, testare e installare gli aggiornamenti necessari per le applicazioni, per i driver e per il sistema operativo dei computer.

[15] Un gateway di sicurezza (spesso chiamato anche firewall) è un sistema di dispositivi e programmi che garantisce il collegamento sicuro delle reti IP, limitando la comunicazione tecnicamente possibile a quella definita come regolamentare nelle direttive sulla sicurezza.

Sia l'amministrazione provinciale[16] sia la IAA hanno un proprio disciplinare per l'**uso aziendale e privato dell'internet e della posta elettronica**.

IV. Valutazioni e raccomandazioni

La gestione della sicurezza delle informazioni è un **processo continuo**[17], le cui strategie e concezioni devono essere costantemente riviste riguardo all'efficacia e, se necessario, aggiornate. Per questo si devono definire, in modo adeguato e vincolante, le priorità e gli obiettivi di sicurezza, la capacità di far fronte ai rischi e in che misura si è disposti a correrli.[18]

Riguardo a un modello procedurale chiaro, completo e coerente[19], in grado di garantire che nell'amministrazione provinciale la gestione della sicurezza, della continuità e dei rischi avvenga e si sviluppi in modo strategico, sistematico, orientato agli obiettivi, coerente ed efficiente, si esprime la raccomandazione – ai fini della trasparenza e della comprensibilità – di descrivere e formalizzare il **processo di gestione della sicurezza**.

Poiché i requisiti di sicurezza cambiano continuamente ("la sicurezza è un obiettivo mobile"), il processo di gestione della sicurezza dovrebbe includere anche un processo di miglioramento continuo. A questo fine si presta p. es. il ciclo PDCA, noto nella gestione della qualità.[20]

Per definire specificamente per l'amministrazione provinciale gli obiettivi di sicurezza delle informazioni e la strategia di sicurezza si raccomanda di adottare formalmente, ferme restando le prescrizioni dell'Agid, una **direttiva di sicurezza**.

La nomina formale del **responsabile della sicurezza delle informazioni** dovrebbe avvenire al più tardi una volta concluso il processo di sviluppo organizzativo della ripartizione.

La ripartizione riferisce che le **risorse di personale e finanziarie** dedicate alla sicurezza, alla continuità e alla gestione dei rischi ammontano nel 2020 a un milione di euro per le tecnologie di sicurezza (di cui il 70% per realizzare il nuovo centro elaborazione dati di Brunico), più un equivalente a tempo pieno esclusivamente per la gestione dei rischi (compresi i piani di continuità e il ripristino di emergenza). I/Le dirigenti responsabili dovrebbero verificare criticamente se l'utilizzo di tali risorse sia sufficiente ovvero adeguato rispetto alle dimensioni dell'amministrazione provinciale, con diverse migliaia di dipendenti e un gran numero di sistemi informatici.[21]

Particolare attenzione si dovrebbe rivolgere a **rafforzare la consapevolezza riguardo ai rischi e alla**

---

[16] https://www.provincia.bz.it/amministrazione/personale/personale-provincia/sviluppo-formazione/pacchetto-benvenuto/postazione-lavoro-informatica.asp

[17] Secondo lo standard BSI 200-2 il processo di sicurezza consiste nelle seguenti fasi: avvio del processo di sicurezza, elaborazione della linea guida sulla sicurezza delle informazioni, creazione di una struttura organizzativa adeguata per la GSI, elaborazione e realizzazione di una concezione per la sicurezza, mantenimento e miglioramento continuo della sicurezza delle informazioni.

[18] Klaus-Rainer Müller, *IT-Sicherheit mit System*, Springer Vieweg, p. 17.

[19] Ibid., p. 17.

[20] Ibid., p. 723.

[21] Secondo il "2015 Global Study on IT Security Spending & Investments" del Ponemon Institute (maggio 2015), le aziende intervistate in complessivamente 42 Paesi impiegano per la sicurezza informatica circa l'8,2% del bilancio destinato all'ambito informatico. Ibid., p. 23.

sicurezza da parte di dirigenti, collaboratori e collaboratrici. Infatti, i pericoli non sono esclusivamente di natura tecnica, né derivano solo da azioni deliberate: anche l'eventuale ignoranza o negligenza da parte del personale può costituire un notevole potenziale di rischio.[22]

Nel quadro di una valutazione generale basata sui risultati della presente indagine – incentrata sugli aspetti legati alla gestione della sicurezza, all'organizzazione e personale, all'infrastruttura, ai sistemi informatici, alle reti e agli ambiti di applicazione – il grado di maturità[23] del sistema dei controlli interni (SCI**)** nella **gestione della sicurezza, della continuità e dei rischi** nell'amministrazione provinciale risulta essere complessivamente a un buon livello.

Entro il 2022 verrà effettuato un follow-up sui suggerimenti e le raccomandazioni finora espresse.

Si ringrazia infine il direttore della ripartizione informatica, i suoi collaboratori e le sue collaboratrici per la fattiva collaborazione prestata nel corso dell'indagine.

08/10/2021

f.to
Wolfgang Bauer

[22] Vedi nota 9, p. 26. Gli obiettivi e i risultati che ci si attendono da una maggiore consapevolezza in materia di sicurezza informatica sono definiti anche nel suddetto piano triennale per l'informatica.

[23] Per determinare il grado di maturità dei sistemi di sicurezza informatica esistono vari metodi e modelli. Vedi anche "Reifegradmodell des Sicherheits-, Kontinuitäts- und Risikomanagements", in Klaus-Rainer Müller, *IT-Sicherheit mit System*, Springer Vieweg, pp. 713 sgg.

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

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

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