DOCUMENTO FUNZIONALE

Strategic PA

CONTROLLO
STRATEGICO
NELLA PUBBLICA
AMMINISTRAZIONE

LA PIATTAFORMA APPLICATIVA PER IL CONTROLLO STRATEGICO

www.strategicpa.it

STRATEGIC PA® UNA PIATTAFORMA APPLICATIVA PER IL CONTROLLO STRATEGICO

INTRODUZIONE

Strategic PA® è impostata per soddisfare a pieno le esigenze per il Controllo Strategico di un Ente Pubblico. Infatti, grazie alla completezza di report e di analisi presenti permette al management dell'Ente di monitorare e controllare le missioni affidate in base agli scostamenti sulle risorse finanziarie e sul personale diretto.

L'analisi avviene mediante l'utilizzo di dashboard, semplici da utilizzare personalizzabili e distribuibili via web.

Strategic PA® è una piattaforma applicativa che integra le funzioni di Performance Budgeting, Obiettivi e Performance, Obiettivi e Indicatori comuni in Blockchain, Anticorruzione e Trasparenza e Società Partecipate. Permette di avere, in una unica visione d'insieme, un controllo a 360° sulle informazioni Economiche, Quantitative e Qualitative presenti all'interno dell'Ente. Ogni modulo è utilizzabile in modo indipendente dagli altri, a meno delle integrazioni funzionali tra i diversi moduli.

Strategic PA® è stato concepito e implementato seguendo i seguenti driver:

- Architettura **Web-Based**
- **Flessibilità, scalabilità** per una migliore gestione e manutenzione evolutiva del prodotto
- Tecnologia di tipo relazionale RDBMS e di tipo **Business Intelligence**
- Flessibilità nelle **personalizzazioni** in base alla metodologia/regolamento dell'ENTE
- **Semplicità** e **rapidità** nella creazione di visualizzazioni di analisi
- **Report di analisi esportabili** nei formati standard (html, xml, pdf, ecc.)
- Integrazione con l'**Active Directory** Aziendale
- Possibilità di generare documenti in ambiente MS Word integrando i dati presenti.
- Utilizzo di tecnologia avanzata per la gestione di cruscotti di analisi avanzati

SICUREZZA STRATEGIC PA®

INTRODUZIONE

Strategic PA® è una piattaforma cloud applicativa efficiente per il controllo strategico nella PA composta da 6 moduli progettati per valorizzare il lavoro, ottimizzare le procedure per il controllo strategico nella Pubblica Amministrazione ed implementa le misure minime di sicurezza previste dalla Circolare Agid n. 2/2017 del 18 aprile 2017 e garantisce il pieno rispetto di quanto previsto dal Reg. EU 2016/679 (GDPR). La qualificazione AGID assicura che l'applicativo fornito in Cloud sia sviluppato e fornito secondo criteri di affidabilità e sicurezza considerati necessari per i servizi digitali pubblici. Tra i requisiti richiesti ci sono:

- la sicurezza applicativa
- la disponibilità di un adeguato supporto tecnico per il cliente
- la trasparenza e la disponibilità di informazioni dettagliate e aggiornate sulle modalità di erogazione del servizio e di esportazione dei dati;
- la disponibilità di incident report, statistiche e strumenti di monitoraggio
- un insieme minimo di livelli di servizio garantiti obbligatori
- la protezione dei dati e la portabilità in tutte le fasi di avanzamento della fornitura

In questo documento vengono descritti i punti di maggiore attenzione sulla sicurezza del servizio.

BACKUP

I dati presenti su Strategic PA® sono localizzati su Data Center certificati Amazon AWS in territorio europeo (region di Francoforte, Germania) e vengono conservati attraverso procedure che prevedono sia il backup delle macchine virtuali, tramite creazione di snapshot, che il backup dei dati su storage sicuro e scalabile in alta disponibilità.

ELEVATA DISPONIBILITÀ E DISASTER RECOVERY

L'elevata disponibilità dei servizi di database di Strategic PA® sono garantiti dall'implementazione Multi-AZ (Zone di Disponibilità Multiple) di Amazon AWS che consente di eseguire carichi di lavoro mission critical con failover automatizzato integrato dal database primario su un database secondario replicato in caso di interruzioni pianificate o impreviste.

Il **Disaster Recovery** di tutta la piattaforma applicativa è implementato tramite un secondo Data Center (Availability Zone) di Francoforte, geograficamente separato dal Data Center primario che

ospita Strategic PA®, dove in caso di interruzioni pianificate o impreviste, si interviene eseguendo ripristino della copia di backup più recente.

DR AUTOMATICO (IN ROADMAP)

I disastri informatici quali guasti nei Data Center, corruzioni a livello server o cyber attacchi possono causare la perdita di dati. Il Disaster Recovery automatico riduce al minimo i tempi di interruzione e la perdita di dati garantendo un ripristino veloce e affidabile tra regioni diverse, in un'area di staging di riferimento e nella tua regione designata. In caso di disastro, in maniera automatizzata è possibile lanciare automaticamente il ripristino sul Data Center di un'altra region nell'arco di pochi minuti.

SISTEMA DI AUTENTICAZIONE

L'accesso al sistema avviene attraverso utenza nominale e password.

Strategic PA® prevede un sistema di gestione delle password previsto dalla legge sulla privacy D.lgs. 196/2003:

- password di almeno 8 caratteri (composta da numeri lettere e simboli speciali)
- password criptata con algoritmo SHA512

Strategic PA® è dotato di opportuni meccanismi per garantire e salvaguardare l'integrità e la sicurezza dei dati in conformità alle disposizioni vigenti in materia. In merito alle autenticazioni, la soluzione offerta recepisce le indicazioni previste nella Circolare Agid n.2/2017:

- accesso ritardato a seguito di tentativi errati
- scadenza password

STRONG AUTHENTICATION

Strategic PA®, seguendo le linee guida adottate da AgID per SPID, ha scelto **OpenID Connect** come standard per tutti i clienti che vorranno integrare l'autenticazione con il proprio sistema di Single Sign On (SSO), consentendo agli utenti di autenticarsi con la propria identità digitale in sicurezza, come descritto nelle linee guida SPID redatte da AgID:

https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2021/12/06/openid-connect-spid-adottate-linee-guida

OpenID Connect è lo standard di autenticazione attualmente utilizzato dalla quasi totalità delle moderne applicazioni web e mobile nel mondo privato le cui caratteristiche rispetto allo standard attualmente utilizzato da SPID (SAML) sono:

- maggiore sicurezza;
- migliore integrazione in sistemi eterogenei (web, mobile, single-page app, IoT e backend);
- maggiore semplicità d'implementazione sicura di componentistica di terze parti;
- interoperabilità;

- scalabilità;
- controlli di sicurezza obbligatori;
- facilità di integrazione.

In roadmap con i nuovi rilasci sono previste le seguenti evolutive:

Possibilità per l'ente di abilitare l'autenticazione forte tramite Multi Factor Authentication (MFA) che prevede l'invio di codici OTP (One time Password) via e-mail o app mobili di sicurezza

PRIVACY DEI DATI

L'audit degli accessi effettuati dagli utenti ai contenuti, è consentito agli amministratori tramite file di log di Strategic PA®.

CRITTOGRAFIA DATI SENSIBILI (IN ROADMAP)

Il sistema, in base al ruolo dell'utente, sarà in grado di garantire la privacy dei dati, in particolare solo gli account autorizzati hanno la possibilità di rendere trasparente o criptato uno specifico dato sensibile.

Il sistema implementerà uno step maggiore di sicurezza che permetterà di ridurre il rischio di violazione dei dati, semplificando la compliance con le soluzioni di crittografia quali:

- gestione delle chiavi
- mascheramento dei dati

MONITORAGGIO

Sono presenti funzionalità di "controllo log di accesso" e di "controllo log di navigazione", verificabili da utenti amministratori dell'applicazione, tenendo traccia delle attività e degli accessi degli utenti.

L'uptime del Data Center è controllato tramite un software di terze parti che mette a disposizione dashboard per la visualizzazione interattiva dei tempi di up e down delle macchine virtuali ed invia alert nel caso in cui il Data Center risultasse irraggiungibile.

VERIFICA DELLA SICUREZZA INFRASTRUTTURALE

La verifica periodica sulla sicurezza dell'infrastruttura viene effettuata dal team ISEC di Ecoh Media formato da esperti di IT security ed è garantita con le seguenti modalità:

- Verifica di nuove patch e fix di sicurezza (sia di sistema che applicative) e relativa installazione con periodicità mensile
- Test periodico di vulnerabilità OWASP (vulnerability assestment)
- Compilazione del CSA STAR Self-Assessment2 (nella versione CAIQ) con ricorrenza annuale, pubblicata sul sito, accessibile tramite questo link.

SICUREZZA INFRASTRUTTURALE

La protezione attiva del Data Center è garantita dai sistemi di sicurezza di Amazon quali ad esempio il Load Balancer di EC2, che consente di non esporre direttamente i servizi e filtrare eventuali tentativi di attacco come DDoS.

Il Load Balancer, inoltre, consente di avere più connessioni di rete ridondate per evitare l'irraggiungibilità dell'applicativo in caso di guasti sulle linee internet del provider.

CONTAINER DOCKER (IN ROADMAP)

Il servizio di Container Docker permetterà una maggiore sicurezza, affidabilità e scalabilità fornendo un solido isolamento di sicurezza tra i contenitori e garantendo che siano in esecuzione i più recenti aggiornamenti di sicurezza.

Strategic PA
CONTROLLO STRATEGICO NELLA PUBBLICA AMMINISTRAZIONE

www.strategicpa.it
è un PRODOTTO di

ECOH MEDIA

ECOH MEDIA S.r.l.
P. IVA 01448300689
N° R.E.A. 96954
info@ecohmedia.com
www.ecohmedia.com

PESCARA

La sede di Spoltore (PE) è situata nel Centro Multiservizi L'Arca: una moderna struttura che guarda a 360° le montagne e il mare.

Via Fellini, 2
65010 Spoltore (PE)
tel. 085 9431161

ROMA

La sede di Roma è situata nel quartiere EUR, in una delle zone più dinamiche della città.

Viale Luca Gaurico 91/93
00143 Roma (RM)
tel. 06 98381868

VARESE

La sede di Gallarate (VA) è situata a pochi chilometri dall'aeroporto di Milano Malpensa.

Corso Sempione 15/A
21013 Gallarate (VA)
tel. 0331 259880