DOCUMENTO DI SPECIFICHE

Strategic PA®
Controllo Strategico

SICUREZZA IN
STRATEGIC PA® | CONTROLLO STRATEGICO

www.strategicpa.it

SICUREZZA STRATEGIC PA® | CONTROLLO STRATEGICO

INTRODUZIONE

Strategic PA® | Controllo Strategico è una piattaforma Cloud applicativa efficiente per il controllo strategico nella PA composta da moduli progettati per valorizzare il lavoro e ottimizzare le procedure per il controllo strategico nella Pubblica Amministrazione.

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.

La piattaforma **Strategic PA® | Controllo Strategico in Cloud** prevede aggiornamenti rivolti a favorire la **security e la privacy** anche nel rispetto delle stringenti normative europee in accordo alle Norme ISO/IEC 27001 – ISO/IEC 27017 – ISO/IEC 27018; a tal proposito è in corso l'iter di certificazione per le norme indicate ai fini del rinnovo della qualificazione AGID.

In relazione ai requisiti del **Regolamento Agid recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi Cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi Cloud per la pubblica amministrazione** e delle norme tecniche indicate, di seguito sono specificate le caratteristiche di sicurezza della soluzione offerta.

CARATTERISTICHE TECNICHE DELLA SOLUZIONE OFFERTA

La piattaforma **IaaS** certificata AGID scelta da Strategic PA® | Controllo Strategico è: **AWS – Amazon Web Service**, leader a livello mondiale (AWS nominata come leader del Cloud per il 10° anno consecutivo nel Magic Quadrant di Gartner per l'infrastruttura e i servizi di piattaforma) e garantisce livelli di continuità, sicurezza e performance elevati a cui si sono affidati grandi aziende internazionali e Enti governativi. (Per il dettaglio delle certificazioni in possesso della piattaforma si faccia riferimento al sito https://aws.amazon.com/it/compliance/iso-certified/).

L'intera infrastruttura applicativa è ospitata presso i Data Center di Amazon AWS in Germania a Francoforte, garantendoci un livello di servizio (SLA) sull'infrastruttura del 99,5 % e inoltre:

- I dati vengono conservati attraverso procedure che prevedono sia il backup delle macchine virtuali che del Data Base
- Tutti i Sistemi Operativi e i relativi Data Base sono **amministrati e aggiornati** dallo staff di sistemisti esperti di Ecoh Media.
- Tutte le componenti software della soluzione Strategic PA® | Controllo Strategico sono costantemente **monitorati e gli eventi sono raccolti e analizzati** dal nostro staff di programmatori per prevenire ogni anomalia applicativa.

La tecnologia **Data Base** utilizzata da Strategic PA® | Controllo Strategico è **Oracle DB**, continuamente aggiornata per garantire i massimi livelli di sicurezza. La nuova versione del DB Oracle prevede una serie di correzioni e patch di sicurezza rispetto alle precedenti. Implementa inoltre, la possibilità di containerizzazione dei database, rendendo la gestione e la manutenibilità più efficienti e trasparenti per l'utente. Sono state incrementate le performance e la possibilità di utilizzare più RAM e CPU rispetto alla versione precedente. Questo permette un incremento notevole delle prestazioni su grossi carichi di lavoro e rapidità nello smaltire la mole di richieste fatte dal software di BI.

La tecnologia **Tableau** di **Data Visualization** è tra le più potenti e affascinanti piattaforme di Business Intelligence a livello mondiale e particolarmente orientata ad un utilizzo da parte degli utenti finali che possono creare facilmente in piena autonomia le Analisi per la rappresentazione dei dati attraverso report e cruscotti analitici in aggiunta a quelli già a disposizione in Strategic PA® | Controllo Strategico.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Ecoh Media ha definito una politica per la sicurezza delle informazioni relativa alla fornitura e l'utilizzo del proprio servizio Cloud, tenendo conto di quanto segue:

- i requisiti di base in materia di sicurezza delle informazioni applicabili alla progettazione e all'attuazione del servizio Cloud;
- i rischi derivanti dagli addetti autorizzati;
- multi-tenancy e Cloud service customer isolation (inclusa la virtualizzazione);
- accesso alle risorse dei clienti del servizio Cloud;
- procedure di controllo degli accessi;
- comunicazioni ai clienti dei servizi Cloud durante il change Managament;
- sicurezza della virtualizzazione;
- accesso e protezione dei dati dei clienti del servizio Cloud;
- gestione del ciclo di vita degli account dei clienti del servizio Cloud;
- comunicazione di violazioni e orientamenti per la condivisione di informazioni in materia di indagini e indagini forensi.

La politica è a disposizione sul sito di Ecoh Media.

GESTIONE ACCESSI DEGLI UTENTI

GESTIONE DEGLI ACCESSI DEGLI UTENTI

L'accesso al sistema avviene attraverso utenza nominale e password e secondo profili diversi a seconda delle funzionalità assegnate dall'amministratore.

Strategic PA® | Controllo Strategico implementa un sistema di autenticazione integrato e prevede le seguenti misure sulla complessità della password:

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

Strategic PA® | Controllo Strategico 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

Two-Factor Authentication

Opzionalmente è possibile per il cliente abilitare la **Two-Factor Authentication (2FA),** un metodo di autenticazione elettronica in cui ad un utente viene concesso l'accesso a **Strategic PA® | Controllo Strategico** solo dopo aver inserito con successo le proprie credenziali (username e password) e un'ulteriore One-Time Password (OTP) generata da un App di Sicurezza per dispositivi mobili come Google Authenticathor, Microsoft Authenticator o Cisco Duo Mobile.

Autenticazione esterna tramite Single Sign On (SSO) del cliente.

L'accesso avviene tramite un provider di identità esterna (IdP) del cliente che, dopo aver autenticato le credenziali dell'utente, gli permette di accedere automaticamente a **Strategic PA® | Controllo Strategico**.
Strategic PA® | Controllo Strategico, 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.

FUNZIONALITÀ DI "CONTROLLO LOG DI ACCESSO" E DI "CONTROLLO LOG DI NAVIGAZIONE"

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 tramite file di log di Strategic PA® | Controllo Strategico**:**

- tipologia dell'evento
- riferimento temporale
- username di chi ha fatto l'operazione
- indirizzo IP.

UTILIZZO DI PROGRAMMI DI UTILITÀ PRIVILEGIATI

L'applicazione non permette all'utente l'utilizzo di programmi di utilità con il servizio Cloud.

CONTROLLI CRITTOGRAFICI

Per i servizi disponibili su AWS, i log ed i backup sono utilizzate le chiavi generate e gestite dal servizio KMS di AWS (AWS Key Management Service (AWS KMS) | Amazon Web Services (AWS)).

GESTIONE DEL CAMBIAMENTO

In merito alla gestione delle modifiche che potrebbero influire negativamente sul servizio Cloud, Ecoh Media opera nel seguente modo:

- **categorie di modifiche**: le categorie di modifiche gestite sono relative ad aggiornamenti tecnologici e di sicurezza;
- **comunicazione al cliente**: ogni modifica viene pianificata e comunicata al cliente con notifica via mail che prevede:
    - natura della modifica
    - data della modifica
    - inizio e fine prevista dell'attività, nella quale la soluzione potrebbe essere non disponibile.

- **verifica della modifica**: ogni modifica viene testata dallo staff tecnico prima e dopo il rilascio, per valutare la sua corretta implementazione e verificare la funzionalità del software.

GESTIONE DELLA CAPACITÀ

Ecoh Media monitora nel tempo la capacità totale delle risorse dedicate nel servizio cloud per prevenire gli incidenti di sicurezza delle informazioni causati dalla carenza di risorse.

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.

Nell'applicativo della soluzione offerta è disponibile il link per il controllo da parte del cliente sul requisito di uptime della soluzione offerta.

BACKUP

I dati presenti su Strategic PA® | Controllo Strategico 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.

Ecoh Media gestisce il requisito attraverso:

- un servizio di **backup giornaliero** con mantenimento delle copie per 15 giorni
- la predisposizione un **Disaster Recovery** a freddo che, in caso di disastro, garantisce la possibilità di ricostruire l'intero ambiente applicativo e i relativi dati attingendo dalle copie di backup
- la predisposizione, l'implementazione e l'esecuzione di test periodici per verificare:
    - l'integrità dei dati di backup
    - la capacità di ripristinare i dati dal backup nei tempi necessari e concordati
    - i luoghi di conservazione dei dati di backup

Non è previsto l'accesso da parte del cliente della soluzione ai dati di backup.

ELEVATA DISPONIBILITÀ E DISASTER RECOVERY

L'elevata disponibilità dei servizi di database di Strategic PA® | Controllo Strategico 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® | Controllo Strategico**,** dove in caso di interruzioni pianificate o impreviste, si interviene eseguendo ripristino della copia di backup più recente.

SINCRONIZZAZIONE DEGLI OROLOGI

Tutti gli orologi interni delle istanze gestite sugli applicativi sono sincronizzati del tempo sugli NTP server di AWS; in particolare è possibile impostare i riferimenti degli orologi sia in modalità UTC che in time Zone Europe/Rome con il cambio dell'ora legale.

GESTIONE DELLE VULNERABILITÀ TECNICHE

Ecoh Media, nell'ambito dei rapporti con il cliente, comunica allo stesso le informazioni su eventuali vulnerabilità tecniche che possono influire sul servizio Cloud fornito.

PRATICHE DI SVILUPPO SICURO

Sono utlizzate le seguenti prassi:

- Separazione degli ambienti: i sistemi di sviluppo, test e produzione sono separati fisicamente e/o logicamente;
- Test dell'applicazione: l'applicazione è consegnata e portata in produzione/esercizio solo dopo essere stata verificata la rispondenza ai requisiti dati;
- Profili Utenti: utlizzo di profilatura, ruoli e permessi assegnati all'utente in funzione delle attività svolte;
- Rilascio applicativo: l'applicativo viene rilasciato in produzione a seguito dei test eseguiti con esito positivo.

GESTIONE DEGLI INCIDENTI RELATIVI ALLA SICUREZZA DELLE INFORMAZIONI

Ecoh Media ha messo a punto ed adotta una procedura specifica per la gestione degli incidenti relativi alla sicurezza delle informazioni che possono aver impatto sulla soluzione offerta e quindi per il cliente.

In particolare l'incidente è gestito attraverso l'istituzione di un canale di contatto tra le parti, solitamente negli accordi contrattuali, e la notifica dell'incidente con messa a disposizione della documentazione relativa a:

- portata degli incidenti di sicurezza informatica;
- informazioni di contatto per il trattamento delle questioni relative agli incidenti;
- eventuali misure correttive applicabili in caso di incidenti di sicurezza delle informazioni.

PROTEZIONE DELLE REGISTRAZIONI

Tutte le registrazioni raccolte dalle istanze sono protette e archiviate in modo che l'accesso può avvenire solo da parte di persone autorizzate dall'amministratore in funzione dell'utilizzo del servizio da parte del cliente.

ACCESSO VIA BROWSER A STRATEGIC PA® | CONTROLLO STRATEGICO IN CLOUD

Con un semplice Browser da PC, Tablet, Smartphone un utente autorizzato può utilizzare le funzionalità di Strategic PA® | Controllo Strategico sia che si trovi in ufficio, o a casa, o in qualsiasi altra locazione dotata di collegamento Internet.

I Browser compatibili con Strategic PA® | Controllo Strategico:

- Chrome on Windows, Mac
- Microsoft Edge su Windows
- Mozilla Firefox su Windows e Mac
- Apple Safari on Mac

Per quanto riguarda IE11 possono esserci delle incompatibilità con la veste grafica attuale (CSS) che possono essere risolte in fase di attivazione del modulo in produzione.

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 assessment)
- Compilazione del CSA STAR Self-Assessment2 (nella versione CAIQ) con ricorrenza annuale, pubblicata sul sito, accessibile tramite il seguente link:
- https://www.ecohmedia.com/strategicpa/wp-content/uploads/2022/02/CAIQ_v3.1_Ecoh_Media.xlsx

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.

Strategic PA
Controllo Strategico

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