Allegato Sicurezza

pagoPA

Centro Stella

Novembre 2020 - v1.4

INDICE

1 Introduzione

Il Gruppo SIA considera la Sicurezza delle Informazioni un aspetto primario per la protezione del proprio business e dei propri clienti.
Il presente documento contiene e dettaglia i controlli di sicurezza che SIA adotta per garantire la sicurezza delle informazioni.
Esso descrive i controlli di sicurezza:

- A cui SIA allinea, se necessario, tutti i servizi attualmente forniti, se non diversamente specificato.
- Con i quali SIA fornirà tutti i nuovi servizi.

Le misure di sicurezza SIA sono state selezionate utilizzando un approccio basato sul rischio dal punto di vista della sicurezza e della protezione dei dati, compresi gli standard e le leggi tempo per tempo applicabili.
Tali misure includono, a titolo esemplificativo ma non esaustivo, firewall, soluzioni per la protezione dei dati, software di rilevamento delle intrusioni, dispositivi di autenticazione, gestione dei database degli utenti, "robustezza" dei sistemi e dei database.
La reputazione dell'azienda si basa sulle sue risorse fisiche, informative e personali.
Pertanto, per il mantenimento della reputazione aziendale, SIA ha definito un quadro di sicurezza per proteggere i processi e le informazioni aziendali da una vasta gamma di minacce e per ridurre al minimo l'impatto di eventuali minacce sulla continuità delle operazioni.

SIA Group promuove un ambiente di gestione etica e controllata delle informazioni per garantire la conformità normativa e un vantaggio competitivo sul mercato. Questa politica sostiene la costante dedizione di SIA Group alla sicurezza dei dati, delle reti e dei dipendenti.

SIA, per le attività di propria competenza, mantiene, monitora e aggiorna regolarmente la conformità a alle predette misure in base alle disposizioni delle norme ISO / IEC 27001, ISO 22301 e, ove applicabile, lo standard PCI DSS.
Il Cliente è responsabile della conformità dei controlli di sicurezza alle leggi, ai regolamenti e ai contratti di lavoro applicabili al Cliente stesso e a tutte le altre leggi, regolamenti e contratti di lavoro che non rientrano nella responsabilità di SIA ai sensi del presente paragrafo.

Le entità del Gruppo SIA sono certificate rispetto a tutti gli standard applicabili nelle regioni in cui operano e a seconda dei servizi offerti:

PCI-DSS, Professione della carta, PIN e 3DS
ISO/IEC 27001, o ISO 22301

2 Organizzazione della sicurezza informatica

2.1 Struttura del Team

SIA ha istituito un team di Cybersecurity all'interno del proprio gruppo che è incaricato di definire e implementare le regole di sicurezza informatica in tutte le sedi, creando centri di competenza e sfruttando le competenze dei membri di ciascun team. Sotto la direzione del CISO (Chief Information Security Officer) e insieme ai LISO (Local Information Security Officers) ci sono 4 team di professionisti della sicurezza che offrono i loro servizi in tutte le sedi del gruppo SIA.

Questi Centri di Competenza sono:

- Governance, Assurance e Allineamento con focus su tutte e tre le aree della Cyber Security
- Business Partner con particolare attenzione ai progetti di business e all'interazione con i clienti
- Controlli di sicurezza e CERT, che gestisce i controlli strategici, la registrazione e la risposta agli incidenti
- Operazioni di sicurezza che gestisce tutte le attività operative come la gestione delle identità, la gestione delle chiavi, la gestione delle vulnerabilità, ecc.

Tutti i professionisti in materia di sicurezza informatica sono assegnati a un team a seconda delle loro conoscenze ed esperienze, con lo scopo di scegliere le persone migliori per la specifica mansione. SIA si assicura che tali esperti vengano formati e, di conseguenza, certificati per eccellere nei loro compiti quotidiani.

2.2 Ruoli e responsabilità

SIA promuove una cultura digitale consapevole dei rischi sulla sicurezza e sulla privacy.

Una cultura della sicurezza contribuisce all'efficacia del programma di sicurezza delle informazioni; infatti, il programma di sicurezza informatica è più efficace quanto i processi di sicurezza sono profondamente radicati nella cultura di SIA.

Per costruire questa cultura, il sistema di gestione della sicurezza delle informazioni è organizzato con la definizione dei seguenti ruoli e responsabilità:

Comitato di gestione (MC)

Il Comitato Direttivo della Capogruppo supervisionerà l'esecuzione del Cyber Information Security Program di SIA, che è guidato dal Chief Cyber Information Security Officer.

Ufficio Cyber Security

La responsabilità di proteggere le risorse del cyberspazio SIA su base giornaliera è condivisa da ogni dipendente, lavoratore non dipendente e dall'azienda, la specifica autorità di governo per la politica di sicurezza delle informazioni e il supporto di specifiche policy, standard e procedure di sicurezza delle informazioni è affidata al personale dell'ufficio di Cybersecurity che ne detiene la responsabilità generale.

L'ufficio di Cybersecurity è composto da tutti gli impiegati che lavorano nei dipartimenti di Cybersecurity dell'intero gruppo SIA e sono responsibili di:

- Istituire e mantenere il Programma di Cybersecurity di SIA che comprende: Cybersecurity Governance e Rischi, Cybersecurity Compliance e Operazioni di Cybersecurity (Identity and Access Governance, Identity and Access Management, Crittografia dei dati, Gestione delle chiavi e dei certificati, Infrastruttura di sicurezza, Test & Assurance, Incident Management);

- Stabilire e mantenere le policy, gli standard e le procedure di sicurezza delle informazioni di SIA che soddisfano le esigenze di sicurezza informatica di SIA e sono conformi a tutte le leggi e i regolamenti tempo per tempo applicabili;
- Stabilire e mantenere un programma per la gestione del rischio di sicurezza informatica per SIA;
- Stabilire e mantenere un programma per la gestione della conformità alla sicurezza informatica per SIA.

Responsabile della sicurezza informatica (CISO)

- Il Chief Information Security Officer (CISO) stabilisce, implementa, mantiene e fa rispettare il programma di sicurezza informatica di SIA. Ciò include la protezione delle risorse informative contro la modifica, la distruzione o la divulgazione accidentale o non autorizzata degli accessi, attraverso lo sviluppo e l'implementazione di policy, standard, procedure e soluzioni tecniche di sicurezza informatica.
- Le responsabilità includono, a titolo esemplificativo ma non esaustivo, a quanto segue:
    - Fornire un rapporto dettagliato sul rischio di sicurezza informatica, sulla conformità, sui controlli, sulla supervisione, ecc. non meno di una volta all'anno al Comitato Direttivo del Gruppo SIA;
    - Partecipare al Comitato per la Governance dei rischi;
    - Dirigere un'organizzazione di risposta agli incidenti che coordina e supporta le attività di risposta agli incidenti legati alla sicurezza informatica;
    - Assicurare la conformità con le policy, gli standard, i regolamenti e la legislazione in materia di sicurezza informatica, a seconda dei casi;
    - Definire e presiedere il Group Cyber Security Governance Committee e il Group Cyber Security Risk Committee;
    - Supervisionare il programma dei Local Information Security Officers;
    - Stabilire le misure di sicurezza per la gestione del rischio delle informazioni;
    - Sorvegliare tutte le eccezioni a questa policy.
- Nei suoi compiti può essere supportato da un sostituto appositamente nominato.

Responsabile della sicurezza informatica locale (LISO)

Il Local Information Security Officer, è nominato in ogni filiale del Gruppo SIA ed è responsabile della formazione, dell'implementazione e della governance del programma di Cybersecurity e delle relative policy. Le sue responsabilità includono, a titolo esemplificativo ma non esaustivo, a quanto segue:

- Comprendere le aree funzionali del business locale e le esigenze di business e fornire direzione e leadership alla Filiale del Gruppo SIA per l'implementazione della strategia di Cybersecurity allineata alla strategia di Business;
- Prendere parte alle attività di valutazione del rischio legate all'attività quotidiana e ai progetti;
- Agire come principale punto di contatto, come indicato, per le questioni relative alla sicurezza e consentire la valutazione operative;
- Assistere la filiale del Gruppo SIA assegnata con la policy di sicurezza delle informazioni, gli standard e la conformità delle procedure;

- Fornire supporto durante gli incidenti di sicurezza informatica.

3 Rilevazione e gestione delle vulnerabilità

SIA ha stabilito istruzioni operative e linee guida per tutti gli utenti del Gruppo SIA, i proprietari delle informazioni, dei sistemi e delle applicazioni per quanto riguarda i test di penetrazione al fine di descrivere i requisiti di gestione delle vulnerabilità e le normative secondo la Policy di Sicurezza delle Informazioni del Gruppo SIA.

Le Norme si basano sulla Policy di Sicurezza delle Informazioni del Gruppo SIA e fanno parte del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) dell'organizzazione.

L'Ufficio di Cybersecurity è responsabile del monitoraggio delle fonti di sicurezza per le comunicazioni di vulnerabilità, la correzione di patch e non, e le minacce che corrispondono al software all'interno dell'inventario del software organizzativo, incluse le segnalazioni in arrivo dai clienti e originate dal programma di Responsible Disclosure.

L'Ufficio di Cybersecurity è responsabile di:

- Eseguire, in linea con PCI DSS o almeno annualmente, le scansioni delle vulnerabilità dei sistemi esterni ed interni di SIA, e di tracciare e segnalare le vulnerabilità identificate;
- La prioritarizzazione dei sistemi per il ripristino a supporto dei processi di gestione delle vulnerabilità.

Attualmente l'ufficio di Cybersecurity classifica le vulnerabilità in linea con la classificazione CVSS e a seconda del livello di criticità del servizio aziendale impattato. L'ufficio di Cybersecurity categorizza le vulnerabilità in quattro livelli: Critico, Alto, Medio e Basso.

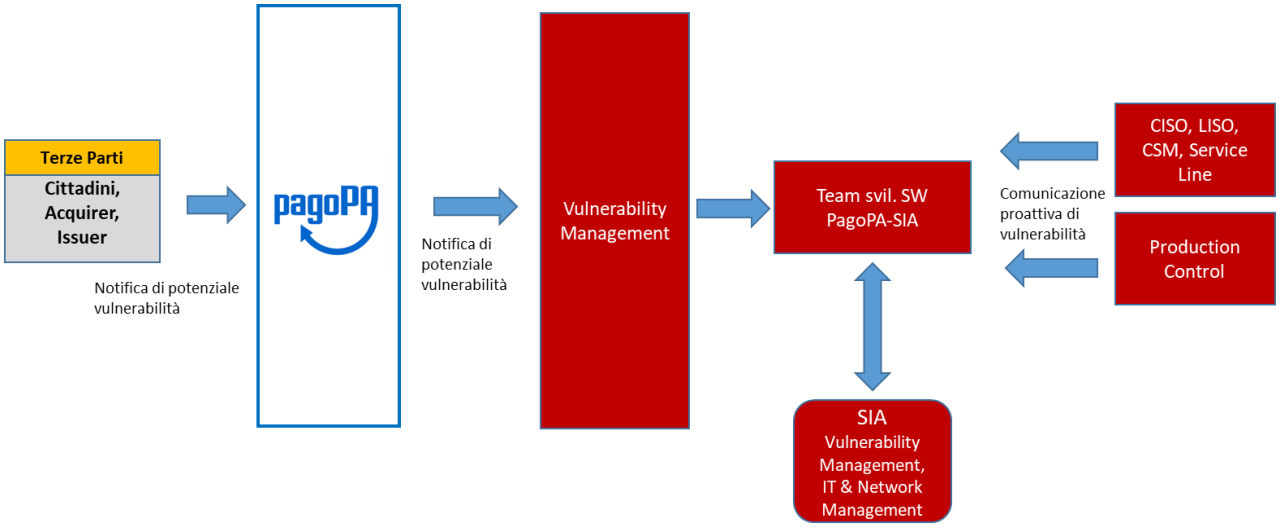
- Se le vulnerabilità sono considerate "Basse" sono mitigate entro novanta (90) giorni dalla notifica;
- Se le vulnerabilità sono considerate "Medie" sono mitigate entro trenta (30) giorni dalla notifica;
- Se le vulnerabilità sono considerate "Elevate" sono mitigate entro sette (7) giorni dalla notifica;
- Se le vulnerabilità sono considerate "Critiche" sono mitigate immediatamente dopo la notifica.

4 Processo di segnalazione

SIA VM gestisce direttamente I controlli del monitoraggio di sicurezza e autonomamente può rilevare delle vulnerabilità.

Se la problematica viene rilevata da una terza parte o da pagoPA, la stessa potrà essere comunicata a SIA da parte di pagoPA attraverso lo strumento di ticketing o in caso di indisponibilità attraverso specifico indirizzo e-mail.

Di seguito viene riportato il flow di processo relativo alle modalità di segnalazione e gestione di una potenziale vulnerabilità.



4.1 Modalità di gestione delle vulnerabilità

Le segnalazioni rilevanti per la sicurezza (come ad esempio quelle ricevute attraverso il programma di *Responsible Disclosure*[1]) sono comunicazioni che vertono sulla segnalazione di potenziali problematiche di sicurezza, comunicate in maniera confidenziale da ricercatori o hacker etici a pagoPA; per questa tipologia di segnalazioni si ha l'esigenza di avere un tempo di presa in carico rapido, una sollecita verifica dell'effettiva o meno veridicità circa la problematica comunicata, ed un tempo di risoluzione certo.

Le metriche utilizzate sono le seguenti:

Metrica	Descrizione	Misurazione
TTO - Time To OWN	Entro quanto tempo dalla ricezione della segnalazione	Dall'arrivo della segnalazione sul sistema di Ticketing.

[1] https://www.pagopa.gov.it/security.html

	l'operatore competente deve prenderla in carico.	
TTA - Time To ANALYZE	Tempo massimo che l'operatore deve impiegare per verificare la veridicità di una segnalazione.	All'interruzione del TTO, sino alla fornitura di un riscontro al cliente.
TTR - Time To RESOLVE	Tempo massimo che l'operatore deve impiegare per la risoluzione della segnalazione oppure per procedere all'inoltro della segnalazione verso il profilo competente.	All'interruzione del TTO, sino alla risoluzione o assegnazione della segnalazione.

Gli step di gestione di una segnalazione rilevante per la sicurezza sono i seguenti:

- il Cliente invia la segnalazione al Fornitore per mezzo email (o altro strumento da concordare) ad opportuno referente SIA, con keyword "RDP" nell'oggetto ed eventuale uso di GPG (da concordare);
- parte il Time To OWN (TTO) in cui il Fornitore la prende in carico dandone evidenza al Cliente (es: risposta alla mail);
- dalla presa in carico parte il Time To ANALYZE (TTA) in cui il Fornitore effettua un'analisi della segnalazione e risponde:
    - confermando il tempo di risoluzione in base alla gravità segnalata (entro il Time To Resolve - TTR);

con una richiesta di rapidi approfondimenti/chiarimenti in merito, ricevuti i quali parte il TTR.

Operativamente, una volta ricevuta la segnalazione, la stessa viene inoltrata ai team tecnici di SIA, i quali verificheranno:

- l'effettiva esistenza di una vulnerabilità;
- la rischiosità della stessa (i.e. cap.3);
- le modalità di intervento;
- le priorità con cui applicarle.

Le Parti concordano che laddove venga accertata una vulnerabilità esclusivamente in carico a SIA, la stessa si impegna a comunicare prontamente al Product Owner di pagoPA il livello di criticità. SIA si impegna altresì ad applicare azioni risolutive attraverso l'approccio della sistemazione che potrà includere la risoluzione della causa (installazione di patch, aggiornamento della versione del software, modifiche alla configurazione, ecc.) o,

laddove l'azione non fosse fattibile, disponibile o richiedesse tempistiche non adeguate, la mitigazione mediante attività / controlli equivalenti (ad esempio, applicazione della regola di sicurezza IPS, applicazione della regola di sicurezza WAF, firewall, ecc.). Tale risoluzione sarà effettuata secondo quanto previsto nel precedente capitolo *"3. Rilevazione e gestione delle vulnerabilità",* ovvero ulteriore diverso termine concordato tra le Parti.

In caso di Vulnerabilità la cui risoluzione non sia dipendente esclusivamente da SIA, le Parti convengono che l'analisi delle stesse e l'eventuale relativa soluzione sarà oggetto di valutazione da parte del Team Tecnico Congiunto coordinato dal Product Owner di pagoPA. Tale condizione non attribuirà a pagoPA il diritto a ricevere alcuna indennità o a pretendere alcun risarcimento di danni ovvero a far valere alcun altro diritto per legge conseguente all'inadempimento.

Le Parti concordano che, laddove il livello di criticità sia classificato Elevato o Critico, ai fini del calcolo delle penali saranno considerati solo i tempi intercorsi sino al rilascio della soluzione che mitiga il rischio connesso alla vulnerabilità, secondo dei parametri concordati con pagoPa.

Le Parti concordano che ove venga accertata una vulnerabilità la cui risoluzione e/o mitigazione possa comportare impatti rilevanti sull'operatività del servizio (es. aggiornamento dei protocolli di cifratura per accedere al servizio e conseguente esclusione degli utenti i cui device non sono compatibili) verrà previsto il coinvolgimento del Product Owner PagoPA per stabilire tempi e modalità circa la mitigazione/risoluzione della vulnerabilità stessa. In tale fattispecie non troveranno applicazione le penali indicate nella tabella dedicata, fermo restando che eventuali ulteriori contestazioni verranno discusse in buona fede tra le Parti nel Service Meeting.

4.2 Livelli di servizio

Viene riportata di seguito la tabella dei livelli di Servizio definiti.

ID (Acronimo) Definizione	Descrizione	SLA (obiettivo)	Metodologia di calcolo / verifica	Unità temporale di calcolo
S-1 (TTOS) Tempo di presa in carico di una segnalazione rilevante per la sicurezza	Indica entro quanto tempo il LIVELLO competente deve prendere in carico una segnalazione rilevante per la sicurezza	100% del totale dei TTOS entro 4h lav.	N/A	Mese
S-2 (TTAS) Tempo di analisi di una segnalazione rilevante per la sicurezza	Indica entro quanto tempo il LIVELLO competente deve riscontrare una segnalazione rilevante per la sicurezza	100% del totale dei TTAS entro 18h lav.	N/A	Mese
S-3 (TTRSC)	Indica entro	100% del totale	N/A	Mese

Tempo di risoluzione di una segnalazione rilevante per la sicurezza di gravità CRITICAL	quanto tempo il LIVELLO competente deve risolvere una segnalazione rilevante per la sicurezza di gravità CRITICAL	dei TTRSC entro 12h lav.		
S-4 (TTRSH) Tempo di risoluzione di una segnalazione rilevante per la sicurezza di gravità HIGH	Indica entro quanto tempo il LIVELLO competente deve risolvere una segnalazione rilevante per la sicurezza di gravità HIGH	100% del totale dei TTRSH entro 30h lav.	N/A	Mese
S-5 (TTRSM) Tempo di risoluzione di una segnalazione rilevante per la sicurezza di gravità MEDIUM	Indica entro quanto tempo il LIVELLO competente deve risolvere una segnalazione rilevante per la sicurezza di gravità MEDIUM	100% del totale dei TTRSM entro 120h lav.	N/A	Mese

4.3 Penali

Fermo restando ove applicabile il risarcimento del maggior danno, le penali previste sono le seguenti:

Codice SLO	Acronimo	Periodo di rilevazione	Penale	Note
S-1	TTOS	Mensile	€500 per ogni ora oltre soglia	
S-2	TTAS	Mensile	€500 per ogni ora oltre soglia	
S-3	TTRSC	Mensile	€200 per ogni ora oltre soglia	
S-4	TTRSH	Mensile	€200 per ogni ora oltre soglia	
S-5	TTRSM	Mensile	€200 per ogni ora oltre soglia	

4.4 Orario lavorativo

Le ore riportate nella tabella degli SLA, vengono calcolate rispetto alle date di calendario come di seguito indicato:

- Le date sono espresse secondo il calendario gregoriano.
- Giorno di calendario (CD – Calendar Day): riferito ad un giorno del Calendario Gregoriano.
- Giorno lavorativo (WD – Working Day): tutti i giorni esclusi sabati, domeniche, 1 gennaio, 6 gennaio, lunedì di Pasqua, 25 Aprile, 1 maggio, 2 giugno, 15 agosto, 1 novembre, 8 dicembre, 25 dicembre e 26 dicembre.
- Orario lavorativo si intende: 08:30 - 18:00] CET da lunedì a venerdì (ad eccezione dei giorni 14 agosto, 24 e 31 Dicembre, per i quali l'orario lavorativo si intende: 08:30 - 13:00)

_____

(luogo e data)

Il Cliente

Firmato digitalmente da: GIUSEPPE VIRGONE
Ruolo: AMMINISTRATORE UNICO
Organizzazione: PAGOPA S.P.A./15376371009
Data: 01/12/2020 12:18:55

Firmato digitalmente da: FEDERICO LOVADINA
Data: 01/12/2020 16:58:13

Firmato digitalmente da: Eugenio Tornaghi
Data: 01/12/2020 16:29:01