	DSI 01	Pagina 1 di 4
	Politica del Sistema per la Gestione della Sicurezza delle Informazioni	rev. n° 2 del 18/12/2019
	Classificazione documento:	PUBBLICO

Premessa

Var Group S.p.A (in seguito Var Group) si propone sul mercato come interlocutore specializzato nell'innovazione tecnologica del settore ITC. L'offerta Var Group trae la sua forza dalla profonda conoscenza dei processi aziendali e dall'integrazione di più elementi. È frutto del lavoro di Business Unit focalizzate nello sviluppo di Soluzioni tecnologiche, Managed & Security Services, ERP & Verticals e Digital Transformation.

In tutti questi ambiti di servizio, Var Group considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo, per l'erogazione di servizi di qualità elevata verso i Clienti e un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo.

L'informazione è ritenuta un asset essenziale per il business aziendale e come tale deve essere protetto. Var Group ha deciso, pertanto, di porre in essere un Sistema di Gestione per la Sicurezza delle Informazioni e di garantire un adeguato livello di sicurezza dei dati e delle informazioni nell'ambito della progettazione, sviluppo ed erogazione dei servizi aziendali, anche attraverso l'identificazione, la valutazione ed il trattamento dei rischi ai quali i servizi stessi sono soggetti.

Il Sistema di Gestione per la Sicurezza per le Informazioni di Var Group definisce un insieme di misure organizzative, tecniche e procedurali a garanzia del soddisfacimento dei sotto elencati requisiti di sicurezza di base:

- **Riservatezza**, ovvero la proprietà dell'informazione di essere nota solo a chi ne ha i privilegi;
- **Integrità**, ovvero la proprietà dell'informazione di essere modificata solo ed esclusivamente da chi ne possiede i privilegi;
- **Disponibilità**, ovvero la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti che ne godono i privilegi.

Indirizzo strategico e dichiarazione della Direzione

Al fine di fornire l'indirizzo generale e strategico di Var Group nel breve, medio e lungo termine, per garantire la tutela e la protezione delle informazioni nell'ambito delle proprie attività in accordo con le indicazioni dello standard UNI CEI ISO/IEC 27001, Var Group ha elaborato la politica in materia di protezione del patrimonio informativo aziendale descritta in questo documento


Per raggiungere gli obiettivi di sicurezza informatica individuati come necessari dalla Direzione aziendale deve essere istituito un Sistema di Gestione della Sicurezza delle Informazioni coerente con la politica che l'azienda intende attuare. Il mantenimento di tale sistema è garantito implementando un processo continuo di **miglioramento** che coinvolga tutte le funzioni aziendali interessate:

- Il personale, che metterà in atto le politiche ed i requisiti di sicurezza per raggiungere gli obiettivi prefissati.
- I clienti, che saranno garantiti per le loro esigenze di sicurezza, in misura conforme agli impegni assunti da Var Group.
- I fornitori, che contribuiranno, in quanto partner, al raggiungimento degli obiettivi dell'organizzazione, e accetteranno le politiche di sicurezza ed i rischi connessi alla fornitura.

La Direzione è consapevole che la realizzazione del Sistema di Gestione richiede uno sforzo iniziale significativo e che il mantenimento e il miglioramento continuo devono essere garantiti da un supporto organizzativo adeguato.

A tale scopo saranno apportate modifiche all'organizzazione di Var Group in modo tale che i ruoli e le responsabilità sulla Sicurezza delle Informazioni siano definiti e siano in grado di operare nella direzione indicata dalla presente politica.

La Direzione renderà disponibili gli investimenti idonei a soddisfare le politiche e gli obiettivi stabiliti e ritiene opportuno affrontare la fase di avvio del Sistema con l'inserimento di risorse esterne che siano in grado di dare il loro supporto qualitativo e quantitativo su tutti gli aspetti inerenti la sicurezza delle informazioni.

	DSI 01	Pagina 2 di 4
	Politica del Sistema per la Gestione della Sicurezza delle Informazioni	rev. n° 2 del 18/12/2019

Questa politica rappresenta gli obiettivi ed i requisiti generali emessi dal management di Var Group che devono essere recepiti dalle strutture aziendali, ciascuna per lo specifico ambito di competenza, affinché l'attività lavorativa sia conforme a quanto specificato nella presente politica.

Valutazione dei rischi e quadro generale dei controlli

I requisiti di sicurezza sono identificati da una valutazione sistematica dei rischi per la sicurezza con metodologie riconosciute da standard internazionali.

I risultati della valutazione dei rischi contribuiranno a determinare le azioni appropriate per la gestione e per l'implementazione dei controlli a protezione contro tali rischi. Ne determineranno anche le relative priorità.

La valutazione dei rischi sarà ripetuta periodicamente per affrontare eventuali cambiamenti che potrebbero influenzare il fattore di rischio.

Dalla valutazione dei rischi i costi dei controlli dovranno essere bilanciati dai benefici della protezione contro i danni che il business potrebbe riportare a seguito di difetti nella sicurezza delle informazioni.

Il Patrimonio Informativo Aziendale

Qualunque tipo di aggregazione di dati che hanno un valore per l'azienda, indipendentemente dalla forma e dalla tecnologia utilizzata per il loro trattamento e conservazione, contribuisce alla formazione del patrimonio informativo dell'azienda. L'informazione deve essere protetta in tutti i possibili formati nei quali è resa disponibile:

- cartaceo (documenti, lettere, elenchi, etc.)
- elettronico (database, dischi, nastri, etc.)
- verbale (riunioni, conversazioni personali e telefoniche, seminari, interviste, etc.)

A seconda della tipologia e dell'origine, le informazioni che costituiscono il Patrimonio Informativo aziendale possono essere suddivise in.

- Informazioni derivanti dal **Patrimonio Informativo del Cliente**, rappresentate dall'insieme delle informazioni gestite da Var Group attraverso i servizi forniti e attualmente localizzati nei Data Center gestiti direttamente o indirettamente dall'azienda. La sicurezza di queste informazioni deve essere garantita per contratto con i Clienti e qualsiasi incidente di sicurezza avrebbe conseguenze dirette sull'immagine e sullo sviluppo del business aziendale
- Informazioni derivanti dal **Patrimonio informativo interno**, rappresentate da tutte le informazioni interne all'azienda ed in parte gestite attraverso i Sistemi Informativi. Queste informazioni hanno influenza sulle altre e condizionano direttamente o indirettamente tutte le attività di business.

Le informazioni devono essere valutate per attribuire loro la relativa importanza a livello del business aziendale al fine di implementare contromisure di sicurezza adeguate e proporzionali alle diverse forme ed alle differenti modalità di interazione utilizzate.


Implementazione del sistema

La presente politica di sicurezza delle informazioni individua gli aspetti di sicurezza da implementare all'interno dell'organizzazione al fine di supportare la missione di Var Group e di perseguire i seguenti obiettivi primari:

Le funzioni aziendali preposte alla gestione e sicurezza delle informazioni hanno il compito di tradurre i sopra citati obiettivi e requisiti generali in contromisure e policy di sicurezza più specifiche, nell'ottica di ottenere un congruo Sistema di Gestione della Sicurezza delle Informazioni.

Gli **obiettivi primari** da perseguire secondo la politica di sicurezza adottata sono i seguenti:

- conformità alle normative vigenti
- salvaguardia dell'immagine aziendale
- protezione del business
- rispetto degli accordi contrattuali
- [mantenimento conformità allo standard UNI CEI ISO/IEC 27001](#)
- [applicazione delle linee guida ISO 27017 e ISO 27018 per i servizi Cloud](#)

	DSI 01	Pagina 3 di 4
	Politica del Sistema per la Gestione della Sicurezza delle Informazioni	rev. n° 2 del 18/12/2019

Tali obiettivi potranno essere raggiunti da Var Group, attraverso la collaborazione di tutte le strutture aziendali ed intergruppo che, ciascuna per la parte di propria competenza, provvederanno ad istituire un sistema di governo della sicurezza in grado di:

- garantire la riservatezza, l'integrità e la disponibilità delle informazioni
- valutare i livelli di rischio
- monitorare i livelli di sicurezza.
- formalizzare i requisiti di sicurezza in conformità alla normativa cogente e alle "best practices" del settore
- garantire un adeguato livello di competenza del personale, raggiunto con la necessaria formazione e addestramento e con la trasmissione della consapevolezza dell'importanza della sicurezza delle informazioni;
- pianificare e gestire la continuità del business;

I contenuti delle indicazioni e delle prescrizioni del sistema si applicano a tutto il personale interno, intergruppo ed esterno, alle aziende partners, ai fornitori ed outsourcers ed a chiunque entra in contatto con le informazioni di proprietà di Var Group.

Tutto il personale che, a titolo di dipendente, consulente o collaboratore, collabora con l'azienda nei processi di progettazione, sviluppo, gestione e controllo dei servizi erogati è responsabile dell'osservanza delle prescrizioni e delle indicazioni del sistema ed è tenuto a proteggere tutte le informazioni trattate durante le proprie attività lavorative. Il personale, consapevole dell'importanza delle informazioni trattate deve agire per garantirne la protezione e provvedere alla segnalazione di anomalie, anche non formalmente codificate, di cui dovesse venire a conoscenza.

Nel caso in cui le regole di sicurezza stabilite siano disattese da dipendenti, consulenti e/o collaboratori dell'Azienda, la Direzione Var Group si riserva di adottare, nel pieno rispetto dei vincoli di legge e contrattuali, le misure più opportune nei confronti dei soggetti trasgressori.

I soggetti esterni che, intrattengono rapporti con Var Group devono garantire il rispetto dei requisiti di sicurezza esplicitati dalla presente politica di sicurezza anche attraverso la sottoscrizione di un "patto di riservatezza" all'atto del conferimento dell'incarico nel caso in cui questo tipo di vincolo non sia espressamente citato nel contratto.

Politica per l'erogazione dei servizi cloud

Var Group è particolarmente sensibile alle problematiche legate alla sicurezza delle informazioni che caratterizzano le modalità tecniche ed operative con cui vengono offerti i propri servizi cloud.

I servizi cloud di Var Group rientrano nella categoria IaaS (Infrastructure-as-a-Service). Var Group, mediante il Data Center proprietario sito in via Piovola 138 – 50053 Empoli (FI) e il Data Center Data4 nella propria disponibilità giuridica sito in Via Monzoro, 101-105 – 20010 Cornaredo (MI), fornisce dunque solo l'infrastruttura di calcolo e l'ambiente di virtualizzazione ed il Cliente ha completa autonomia nello scegliere come utilizzare questo ambiente (quali dati caricarvi e processarvi, per quali scopi e come proteggerli).

- Suddivisione e condivisione delle responsabilità

Var Group ha definito nuove policy e ampliato le proprie procedure già esistenti in conformità al proprio uso dei servizi cloud e, al tempo stesso, a rendere consapevoli i propri utenti finali circa le rispettive responsabilità nella fruizione dei servizi medesimi. In qualità di cloud service provider, Var Group garantisce chiarezza e trasparenza circa i livelli di sicurezza informatica implementati e le responsabilità che su di esso gravano.

- Restituzione e cancellazione delle informazioni del cliente

I contratti di fornitura dei servizi cloud stipulati da Var Group con i clienti specificano le tempistiche di restituzione delle informazioni alla cessazione del rapporto.

- Obblighi di segregazione


Var Group assicura misure di segregazione logica idonee a consentire la separazione delle risorse utilizzate dai propri clienti del servizio cloud, sia da quelle degli altri clienti, sia da quelle utilizzate da Var Group stessa per proprie esigenze di gestione interna.

- Hardening delle virtual machine

Nella configurazione di macchine virtuali, Var Group assicura, per quanto di propria competenza, che siano adottate le misure tecniche adeguate (vedi, anti-malware, logging) per ogni macchina virtuale utilizzata.

- Monitoraggio del servizio

Ai servizi cloud erogati da Var Group sono applicati strumenti efficienti al fine di poter costantemente monitorare specifici aspetti del servizio fruito.

	DSI 01	Pagina 4 di 4
	Politica del Sistema per la Gestione della Sicurezza delle Informazioni	rev. n° 2 del 18/12/2019

- Uniformità nella gestione della sicurezza per le reti virtuali e fisiche

Var Group definisce e documenta una politica di sicurezza delle informazioni per la configurazione della rete virtuale, coerente con la politica di sicurezza delle informazioni per la rete fisica.

Politica per la protezione dei dati personali nel cloud computing

L'impiego di servizi di cloud è divenuto un irrinunciabile driver di efficienza per molte aziende pubbliche e private. Tra i suoi obiettivi primari Var Group ha quello di applicare una modalità strutturata, basata sul privacy by design, per far fronte alle principali questioni giuridiche, sia di natura legale che contrattuale, legate alla gestione dei dati personali in infrastrutture informatiche distribuite seguendo il modello del cloud pubblico.

Per raggiungere tale obiettivo Var Group ha implementato contromisure specifiche basate sui principi internazionali definiti riguardo alla privacy. Questi principi vengono presi come riferimento per guidare la progettazione, lo sviluppo, l'attuazione, il monitoraggio e la misurazione di politiche sulla privacy e controlli della privacy nei servizi di cloud computing.

L'insieme dei rischi specifici connessi all'adozione di soluzioni cloud riguarda sia la sicurezza dei dati e dei processi aziendali, sia la sicurezza dei dati tutelati dalle normative di cui sopra, sia la corretta applicazione di tali normative nel loro complesso e non solo sotto il profilo della sicurezza.

Facendo riferimento al Regolamento Europeo UE 679/2016, l'ambito corretto in cui collocare l'analisi di questi nuovi rischi e l'individuazione delle adeguate contromisure è certamente il processo di identificazione delle misure idonee e preventive di cui all'art. 32 del Regolamento.

Tutti questi aspetti richiedono di essere indirizzati nella definizione del contratto che regola la fornitura dei servizi di cloud computing. La stipula di tale contratto è uno dei cardini della strategia di gestione dei rischi specifici relativi al cloud computing, per la conformità alla normativa e più in generale per la sicurezza dei dati personali.

In particolare, gli aspetti sui quali Var Group ha focalizzato la sua attenzione sono i seguenti:

- Il rispetto di tutti gli obblighi di propria competenza, trattando dati personali in qualità di responsabile del trattamento,
- la possibilità di operare in modo trasparente, in modo che i titolari del trattamento siano certi di aver scelto un fornitore che garantisce adeguate garanzie,
- l'elaborazione di accordi contrattuali con i titolari del trattamento,
- la garanzia per i titolari del trattamento della presenza di un meccanismo che permetta di esercitare il diritto di audit e di verifica di conformità.

Conclusioni

La Politica per la Sicurezza delle Informazioni deve essere sempre coerente con gli obiettivi di business aziendali e pertanto la Direzione si riserva di apportare eventuali modifiche al presente documento in base al conseguimento dei risultati di Var Group alle aspettative di tutte le parti interessate, all'andamento del mercato di riferimento.

In accordo alla Politica della Sicurezza delle Informazioni e con cadenza almeno annuale, la Direzione fisserà gli obiettivi per la Sicurezza utilizzando anche i risultati raggiunti nel corso dell'anno precedente.

Questa politica è stata approvata dalla Direzione Aziendale di Var Group.

Data e firma della direzione 18/12/2019

Giovanni Moriani