CONDIZIONI PER LA SICUREZZA DELLE INFORMAZIONI E PER IL TRATTAMENTO DEI DATI PERSONALI MEDIANTE I SERVIZI CLOUD EROGATI DA DATA CENTER VAR GROUP

CLASSIFICAZIONE DELLE INFORMAZIONI:

☐ Riservata ☐ Interna ☒ Pubblica

☐ COPIA CONTROLLATA ☒ COPIA NON CONTROLLATA

Distribuita al pubblico

Data	Rev. Num.	Stato	Descrizione
04/02/2024	11	In Vigore	Aggiornamento generale dei contenuti

Redatto	*Verificato*	*Approvato*
Ufficio Q&C **Ufficio DL&DP**	**Responsabile Ufficio Q&C** **Responsabile Ufficio DL&DP**	**Responsabile Ufficio Q&C**

Sommario

INTRODUZIONE *4*

1 CONDIZIONI DI SERVIZIO *4*

1.1 AMBITO E RUOLI *4*

1.2 TRATTAMENTO DEI DATI PERSONALI *4*

1.3 SICUREZZA *6*

1.4 SUBAPPALTATORI *6*

1.5 CONFORMITÀ CON PROTEZIONE DEI DATI *7*

1.6 GESTIONE E CANCELLAZIONE DEI DATI *7*

1.7 VIOLAZIONE DELLE INFORMAZIONI E DEI DATI PERSONALI *8*

2 TRASPARENZA VAR GROUP *9*

2.1 SISTEMA PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI *9*

2.2 ACCORDI DI RISERVATEZZA E FORMAZIONE DEL PERSONALE *9*

2.3 ACCESSO FISICO AL DATA CENTER *9*

2.4 POLITICA DI CONTROLLO ACCESSI LOGICI *10*

2.5 MISURE DI SICUREZZA GENERALI ADOTTATE *11*

2.5.1 ACCESSO REMOTO E VPN 11

2.5.2 CONFIGURAZIONE FIREWALL 12

2.5.3 CONFIGURAZIONE ROUTER 13

2.5.4 CONFIGURAZIONE SERVER 13

2.5.5 SICUREZZA DEI NOTEBOOK 14

2.5.6 MONITORAGGIO E SICUREZZA COMPONENTI INFRASTRUTTURALI E RETE 14

2.5.7 PROTEZIONE ANTI DDOS 14

2.5.8 2VULNERABILITY ASSESSMENT & PENETRATION TEST 15

2.6 MISURE DI SICUREZZA ADOTTATE PER LO SPECIFICO SERVIZIO *16*

2.6.1 VIRTUAL PRIVATE SERVER 16

2.6.2 VIRTUAL DATA CENTER 17
2.6.3 SERVIZIO BACKUP APPLICATIVO (AMBIENTI VMWARE E MS HYPER-V) 18
2.6.4 PARTIZIONI IBM POWER i IN CLOUD 19
2.6.5 HOSTING SITI WEB 20
2.6.6 POSTA ELETTRONICA GESTITA - ZIMBRA 20
3 SERVIZIO SaaS - VAR HUB 22
3.1 VAR HUB - AMBITO E RUOLI 22
3.2 VAR HUB - GESTIONE E CANCELLAZIONE DEI DATI 22
3.3 VAR HUB - MISURE DI SICUREZZA ADOTTATE 23
4 CONTATTI VAR GROUP 25
5 CRONOLOGIA DELLE REVISIONI 26

INTRODUZIONE

Var Group, attraverso il presente documento, si propone lo scopo di guidare i propri Clienti nel valutare se il servizio di infrastruttura cloud che desidera utilizzare sia adatto per le attività di elaborazione dati che desidera effettuare.

Nel prosieguo del documento Var Group descriverà le misure di sicurezza adottate per gli asset e gli ambiti di cui è responsabile. Essendo però il Cliente che decide quali dati caricare e processare sui servizi cloud, solo il Cliente potrà determinare quale è il livello di sicurezza più appropriato per gli eventuali dati personali utilizzati.

Var Group incoraggia dunque i propri Clienti a completare la valutazione delle attività di elaborazione dati che intendono effettuare mediante i servizi cloud e la loro conformità in base alla normativa UE di protezione dei dati.

1 CONDIZIONI DI SERVIZIO

1.1 AMBITO E RUOLI

I servizi cloud di Var Group erogati 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), rientrano nelle categorie:

- **IaaS** (Infrastructure-as-a-Service). Var Group, 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);
- **SaaS** (Software-as-a-Service). In questo caso, quindi, la gestione di Var Group non si limita all'infrastruttura fisica e alla piattaforma di virtualizzazione, ma si estende anche ai server virtuali, ai relativi Sistemi Operativi, ed alle applicazioni installate.

Nell'erogazione dei servizi infrastrutturali cloud, Var Group, in quanto Cloud provider, provvede alla conservazione di dati personali per conto del Cliente; di conseguenza si precisa che con riferimento alle operazioni di trattamento sui dati personali connesse all'erogazione del servizio medesimo, Var Group si astiene dal trattare i dati stessi per finalità proprie ed opera nel pieno rispetto della disciplina di cui al Regolamento 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché nel rispetto di quanto statuito dall'Autorità Garante della Protezione dei dati personali. In particolare, nel trattare i dati personali per conto del Cliente, Var Group agisce in qualità di Data Processor (Responsabile del trattamento), per tale intendendosi, ai sensi dell'art. 4, par. 1, punto 8 del Regolamento UE 2016/679, "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

In qualità di Responsabile del trattamento, Var Group, opera nel pieno rispetto dei principi di cui all'art. 5 del Regolamento UE 2016/679, garantendo, in particolare, la liceità, la correttezza e la trasparenza del trattamento ed impegnandosi a circoscrivere le operazioni da compiere sui dati personali ai soli scopi determinati, espliciti e legittimi definiti dal Cliente, Titolare del trattamento dei dati personali.

Nel paragrafo successivo sono illustrati, sommariamente, gli obblighi assunti, ai sensi dell'art. 28 del Regolamento 2016/679, da Var Group in qualità di Responsabile del trattamento.

1.2 TRATTAMENTO DEI DATI PERSONALI

Premesso che a far data dal 27 aprile 2016 è entrato in vigore il Regolamento UE n. 679 sulla protezione delle persone fisiche in relazione al trattamento dei dati personali e alla libera circolazione dei dati medesimi, si precisa che Var Group ha provveduto ad implementare la propria architettura al fine di dare piena attuazione alla normativa

europea, garantendo l'applicazione di un approccio proattivo nel compimento di operazioni di trattamento sui dati personali al fine di assicurare la protezione dei dati medesimi in via preventiva.

Come anticipato (vedi paragrafo 1.1), Var Group, nell'erogazione dei servizi cloud, agisce in qualità di Responsabile del trattamento. In considerazione di tale qualità, si precisa che Var Group si astiene dallo svolgimento di un controllo sui contenuti che il Cliente sceglie di caricare sul servizio cloud e non assume alcun ruolo nel processo decisionale in merito alle finalità e alla modalità di trattamento; la definizione di tali ambiti compete, infatti, al Cliente in quanto Titolare del trattamento.

In qualità di Responsabile del trattamento, Var Group provvede a:

a) Rispettare le disposizioni di cui al Regolamento 679/2016, nonché eventuali e successive modifiche della disciplina legislativa in materia di trattamento dei dati personali e si impegna, altresì, al rispetto dei Provvedimenti dell'Autorità Garante per la protezione dei dati personali;
b) Rispettare le istruzioni impartite dal Cliente con riferimento al trattamento dei dati personali svolto per conto di quest'ultimo ed espressamente individuate all'interno dell'atto di nomina a Responsabile del trattamento (*Data Processing Agreement*) predisposto dal Cliente, così come stabilito ai sensi dell'art. 28 della normativa europea. In particolare, Var Group provvede a garantire la riservatezza del proprio personale autorizzato al trattamento dei dati personali, istruendolo con riferimento alle operazioni da compiere sui dati personali, nonché con riferimento alla disciplina in materia di protezione dei dati medesimi, anche mediante la predisposizione di appositi corsi di formazione periodici.
c) Inoltre Var Group provvede all'adozione di misure di sicurezza volte a proteggere i dati personali dai rischi di distruzione, perdita, modifica, divulgazione non autorizzata, accesso accidentale o illegale; a tal fine ed in considerazione di quanto statuito nell'atto di nomina Responsabile del Trattamento, Var Group garantisce al Cliente l'adozione di un livello di protezione dei dati personali quanto meno equipollente a quello previsto dal Cliente medesimo, Titolare del trattamento, ed assicura la propria collaborazione qualora quest'ultimo richieda l'integrazione delle misure di sicurezza applicate.
d) È altresì garantita la restituzione dei dati personali e delle eventuali copie dei dati medesimi all'atto di scadenza del vincolo contrattuale con il Cliente, ovvero, in alternativa e su richiesta del Cliente, Var Group provvede a cancellare i dati personali all'atto di scadenza del rapporto contrattuale o, anteriormente a tale momento, in considerazione delle istruzioni impartite dal Cliente. Si precisa che i dati personali non vengono, in nessun caso, copiati o duplicati, salvo l'ipotesi in cui tali operazioni siano state richieste espressamente dal Cliente.
e) Si precisa che Var Group collabora con il Cliente per l'adempimento degli obblighi connessi alla comunicazione dell'eventuale violazione di dati personali (*data breach*), nonché allo svolgimento della valutazione di impatto ai sensi dell'art. 35 del Regolamento UE 2016/679 e dell'eventuale consultazione preventiva ai sensi dell'art. 36 della normativa medesima.
f) Il ricorso a Sub-Responsabili del trattamento avviene in conformità a quanto specificato di seguito (vedi paragrafo 1.4).
g) Rispettare un generale "onere di informazione" nei confronti del Cliente, con riferimento alle operazioni di trattamento dei dati personali, garantendo a quest'ultimo la conoscenza di qualsiasi informazione rilevante in materia di trattamento dei dati personali e provvedendo a fornire tutte le indicazioni volte a comprovare la conformità delle operazioni di trattamento poste in essere alla normativa in materia di protezione dei dati personali e alle istruzioni impartite dal Titolare medesimo. Si precisa che qualora le istruzioni fornite dal Cliente in materia di trattamento dei dati personali appaiano in violazione delle relative previsioni normative Var Group si astiene dal dare esecuzione alle relative operazioni e provvede a dare comunicazione della suddetta violazione al Cliente.
h) Resta inteso che Var Group si rende disponibile a sottoporsi ad eventuali ispezioni o misure analoghe condotte dal Cliente al fine di dimostrare la rispondenza del proprio impianto alla normativa europea in materia di trattamento dei dati personali, nonché alle istruzioni impartite dal Cliente medesimo.

1.3 SICUREZZA

Var Group si impegna ad implementare e mantenere adeguate misure tecniche ed organizzative per le strutture di Data Center, i server, gli apparati di rete ed i sistemi che sono sotto il proprio controllo e vengono utilizzati per l'erogazione dei servizi cloud.

Nell'utilizzo dei servizi IaaS il Cliente è responsabile della sicurezza dei sistemi operativi, delle applicazioni ospitate sul servizio, dei dati in transito e conservati, delle credenziali di accesso al servizio del Cliente e delle politiche di gestione dei permessi per il personale del Cliente che utilizza il servizio.

Nell'utilizzo dei servizi SaaS il Cliente è responsabile della sicurezza delle credenziali di accesso al servizio del Cliente e delle politiche di gestione dei permessi per il personale del Cliente che utilizza il servizio.

Si invitano quindi i Clienti ad esaminare le informazioni relative alla sicurezza dei dati rese disponibili da Var Group, la configurazione del servizio scelta e le misure di sicurezza che il Cliente stesso implementerà per gli aspetti di sicurezza sotto la sua responsabilità e valutare se l'insieme di queste fornisce un livello di sicurezza appropriato per le proprie esigenze. Essendo infatti il Cliente che decide quali dati caricare e processare sui servizi cloud, solo il Cliente potrà determinare quale è il livello di sicurezza più appropriato per gli eventuali dati personali utilizzati.

Var Group è in possesso della certificazione ISO/IEC 27001 dal 2013, adeguata nel 2024 alla nuova versione ISO/IEC 27001:2022. Inoltre, dal 2020 il certificato di sistema di gestione della sicurezza delle informazioni è stato integrato per essere conforme con le linee guida ISO/IEC 27017 (che fornisce linee guida per i controlli di sicurezza delle informazioni applicabili alla fornitura e all'utilizzo di servizi cloud) e ISO/IEC 27018 (codice di condotta incentrato sulla protezione dei dati personali nel cloud).

Le certificazioni sopra citate possono essere visionate all'interno del sito istituzionale www.vargroup.it

Come richiesto da tale norma, Var Group, nei siti da cui eroga servizi cloud:

- Si impegna a mantenere attivo un programma di sicurezza delle informazioni, con l'obiettivo di identificare rischi ragionevolmente prevedibili e interni per la sicurezza della propria rete e minimizzare i rischi per la sicurezza, anche attraverso analisi del rischio e verifiche periodiche (rif. Paragrafo 2.1).
- Garantisce la riservatezza del personale autorizzato a trattare i dati personali del Cliente e a tal fine suddetto personale sottoscrive un apposito atto di designazione e la sua attività è veicolata mediante specifiche indicazioni impartite da Var Group, la quale, come già precisato, provvede ad istruire, periodicamente, il proprio personale in merito alla conoscenza dei contenuti sulla normativa privacy tramite appositi corsi di formazione (rif. Paragrafo 2.2).
- Utilizza politiche e controlli di accesso ai servizi, al fine di limitare l'accesso Var Group al solo personale che necessita di trattare i dati dei Clienti per fornire i servizi contrattualizzati. Allo stesso modo attua politiche di revoca dei permessi quando il personale non necessita più di accedere ai dati del Cliente (rif. Paragrafo 2.4).

1.4 SUBAPPALTATORI

Si precisa che nell'erogazione dei servizi cloud Var Group si avvale di società controllate ai sensi dell'articolo 2359 c.c. e si impegna a non demandare i servizi oggetto del contratto in essere con il Cliente a ulteriori Subappaltatori non appartenenti al gruppo Var Group, salvo sussista specifica autorizzazione scritta del Cliente in tal senso.

Qualora intervengano Subappaltatori non appartenenti al gruppo Var Group nell'erogazione dei servizi cloud al Cliente, Var Group si impegna a dichiararli al cliente all'atto di nomina a Responsabile esterno del trattamento dei dati ed a predisporre e a mantenere aggiornato un elenco dei medesimi; il relativo elenco potrà essere esibito su richiesta del Cliente.

Inoltre, si precisa che tutti i Subappaltatori, agenti per conto di Var Group e nell'interesse del Cliente, sono nominati da Var Group Sub-Responsabili del trattamento dei dati personali, ai sensi dell'art. 28 del Regolamento UE 2016/679, mediante apposito atto giuridico che riproduce i contenuti e gli obblighi dell'atto mediante cui Var Group è stata nominata Responsabile del trattamento dal Cliente.

Var Group mantiene indenne il Cliente, Titolare del trattamento, in relazione a qualsiasi danno, incluse le spese legali, connesso alle operazioni di trattamento dei dati personali e che sia imputabile a una condotta, commissiva o omissiva, del Sub-Responsabile del trattamento.

1.5 CONFORMITÀ CON PROTEZIONE DEI DATI

Var Group si impegna a mettere a disposizione del Cliente tutte le informazioni necessarie a dimostrare la conformità ai suoi obblighi in materia di protezione dei dati e consentire verifiche da parte del Cliente o di un revisore da esso incaricato.

Var Group fornirà dunque ai Clienti che avranno domande riguardanti la protezione dei dati o problemi di sicurezza relativi al servizio tutti i riferimenti necessari per essere messi in contatto con il personale Var Group o con il rappresentante attualmente in carica per gestire tali questioni (rif. Paragrafo 4).

Le infrastrutture da cui Var Group eroga i propri servizi cloud sono costituite da ambienti multi-tenant, condivisi cioè da più Clienti. L'accesso fisico a tali ambienti da parte del singolo Cliente o di una terza parte introduce un potenziale rischio di sicurezza per tutti gli altri Clienti Var Group i cui dati sono ospitati all'interno dello stesso ambiente. Questo rischio può essere controllato se, invece di una verifica in loco, i Clienti utilizzano le informazioni fornite da Var Group per verificarne ragionevolmente la conformità alle misure di sicurezza che si ritengono necessarie.

1.6 GESTIONE E CANCELLAZIONE DEI DATI

Var Group si impegna a fornire per tutta la durata contrattuale al Cliente la possibilità di correggere, cancellare o recuperare i propri dati. Il Cliente potrà utilizzare questa capacità per recuperare o eliminare i propri dati dei Clienti al termine della fornitura di servizio.

Var Group non è tenuta a fornire ulteriore assistenza al Cliente sulla gestione dei dati. Questo perché il Cliente (e non Var Group) è responsabile della gestione dei dati trattati mediante il servizio contrattualizzato.

Alla cessazione del contratto tra le parti, per qualsiasi ragione essa avvenga, Var Group potrà sospendere il relativo servizio senza ulteriore preavviso. I dati del Cliente verranno conservati e resi disponibili per la restituzione per un periodo di 30 gg dalla cessazione; decorso invano tale periodo senza che il Cliente si sia attivato per la restituzione, i dati (compresi i file temporanei) verranno definitivamente cancellati.

Var Group non procede al trasferimento dei dati personali in altri Data Center localizzati in Paesi extra-UE; tuttavia, qualora vi sia specifica indicazione in tal senso da parte del Cliente, Var Group provvede al trasferimento dei dati personali nel pieno rispetto delle istruzioni impartite dal Cliente medesimo all'interno dell'atto di nomina a Responsabile del trattamento e comunque in ossequio alla normativa europea in materia di protezione dei dati personali.

In particolare, Var Group provvede all'eventuale trasferimento di dati personali in Paesi extra-UE esclusivamente in considerazione dell'esistenza di una decisione di adeguatezza della Commissione Europea sul livello di protezione predisposto per i dati personali del Paese terzo, ovvero sulla base di clausole contrattuali modello, debitamente adottate, o di norme vincolanti d'impresa approvate attraverso la specifica procedura di cui all'art. 47 del Regolamento UE 2016/679.

Si precisa altresì che, qualora dovesse sussistere un obbligo giuridico al trasferimento dei dati personali in Paesi extra-UE, pur in mancanza di specifica indicazione in tal senso da parte del Cliente, Var Group, in qualità di Responsabile del trattamento, provvede ad informare quest'ultimo con riguardo all'obbligo medesimo.

1.7 VIOLAZIONE DELLE INFORMAZIONI E DEI DATI PERSONALI

Var Group si impegna a comunicare al Cliente eventuali violazioni delle informazioni e dei dati personali (c.d. "*Data Breach*") in maniera tempestiva e al più tardi entro 24h dal momento in cui ne viene a conoscenza, contattando i riferimenti tecnici del Cliente forniti al momento della contrattualizzazione del servizio e fornendo informazioni circa:

- La natura della violazione avvenuta.
- Le conseguenze generate da tale violazione.
- Le misure adottate o che Var Group propone di adottare (per quanto di sua competenza) in risposta alla violazione avvenuta.
- I contatti (nominativo, mail, telefono) della persona Var Group di riferimento in base al servizio su cui si è verificata la violazione.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente alla prima comunicazione, le informazioni verranno fornite in fasi successive senza ulteriore ingiustificato ritardo.

2 TRASPARENZA VAR GROUP

2.1 SISTEMA PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

L'adozione di un Sistema per la Gestione della Sicurezza delle Informazioni (SGSI) è una decisione strategica dell'Azienda. Per questo motivo Var Group ha deciso di progettare e implementare tale sistema sulla base delle linee guida indicate dalla norma UNI CEI ISO/IEC 27001 integrata con le estensioni 27017 e 27018.

2.2 ACCORDI DI RISERVATEZZA E FORMAZIONE DEL PERSONALE

Var Group stabilisce con i propri operatori delle condizioni di impiego che si basano sul mantenimento di un rapporto di professionalità, competenza e riservatezza.

Al momento dell'impiego qualsiasi operatore, sia esso di nuova assunzione che proveniente da una delle aziende del gruppo Var Group, viene valutato dalle Risorse Umane di Var Group, oltre che dal Responsabile Tecnico di riferimento, per la propria competenza ed esperienza e ad esso viene richiesto di accettare il vincolo di riservatezza con la società assuntrice anche dopo il termine del rapporto di lavoro.

Viene richiesto inoltre di effettuare gli specifici corsi in materia di protezione dei dati personali e di sicurezza delle informazioni e di prendere visione del regolamento aziendale sull'utilizzo dei sistemi informativi, degli applicativi aziendali e delle risorse informatiche, del codice di comportamento, del codice etico aziendale e delle Policy rilevanti che gli vengono messe a disposizione.

2.3 ACCESSO FISICO AL DATA CENTER

Il presente paragrafo si limita a descrivere le modalità con cui Var Group gestisce gli accessi fisici ai propri Data Center utilizzati per l'erogazione dei propri servizi cloud. Per i livelli di servizio dei Data Center si fa invece rimando a *SLA Data Center Var Group* visionabili dal sito istituzionale www.vargroup.it.

L'edificio che ospita il Data Center Var Group è recintato e video-sorvegliato per tutto il perimetro. Gli apparati di video sorveglianza sono attivi 24x7x365 e direttamente collegati con l'istituto di vigilanza privata che garantisce l'intervento in caso di necessità. Nell'edificio è in funzione un sistema di anti-intrusione, con allarmi volumetrici.

Il Data Center Data4 utilizza gli stessi sistemi di video-sorveglianza e di anti-intrusione, con in aggiunta un presidio in loco 24x7 della vigilanza privata.

L'ingresso agli edifici che ospitano i Data Center è permesso solo a seguito del passaggio da un'area di reception presso la quale si provvede al riconoscimento delle persone.

Gli ingressi delle persone ai Data Center sono regolati e controllati tramite lettura di badge di riconoscimento e passaggio attraverso tornelli. L'accesso a questi ambienti è limitato alle persone che vi devono accedere per motivi lavorativi.

Tutto il personale Var Group interno coinvolto, nella manutenzione del Data Center di Empoli o nella gestione dell'operatività dei servizi erogati da entrambi i Data Center, è in possesso di apposito badge personale che garantisce l'accessibilità 24x7 ai locali di competenza con le proprie responsabilità. Periodicamente, con una frequenza almeno annuale, verrà eseguita da parte del responsabile del personale una verifica sui badge personali attivi valutando, ove vi fosse l'esigenza, la richiesta di riconsegna da parte del possessore o la disabilitazione.

Il personale esterno può accedere ai Data Center solo se accompagnato da almeno una persona interna incaricata, e solo a seguito dell'identificazione e registrazione da parte del personale della reception. L'accesso di visitatori

all'area dati di pertinenza Var Group all'interno del Data Center Data4 richiede l'approvazione del Responsabile Tecnico Var Group che si interfaccerà con Data4 stessa per comunicare preventivamente i nominativi esterni.

La registrazione del visitatore può essere effettuata con l'ausilio di un software applicativo in cui l'operatore della reception inserisce le generalità del visitatore, gli estremi del documento d'identità, i dati di entrata e uscita e le coordinate del badge consegnato.

Al visitatore:

- All'atto di registrazione, viene resa apposita informativa, ai sensi dell'art. 13 del Regolamento UE 2016/679, in ordine al trattamento dei dati personali ed è conferita visione dell'elenco delle regole comportamentali da tenere all'interno del Data Center.
- Viene richiesto di apporre una firma per concedere il consenso al trattamento dei propri dati.
- Viene consegnato un badge temporaneo che deve essere restituito all'uscita.
- Al momento della restituzione, l'operatore della reception provvede a ricercare la registrazione dell'ingresso sul software applicativo e chiudere la visita immettendo l'orario di uscita del visitatore.

L'ingresso degli operatori delle linee di comunicazione viene gestito tramite la consegna di apposito badge che permette l'accesso solo limitatamente ad un'area specifica del Data Center, separata dall'area dati.

Al momento dell'uscita dall'edificio, i fornitori devono passare dall'area reception per la riconsegna del badge. Il personale della reception ha cura di registrare le riconsegne e gli orari di uscita.

Le operazioni di carico e scarico del materiale all'interno di Var Group sono effettuate sotto la supervisione di personale interno. Il materiale deve passare attraverso un sistema doppio di varchi ad apertura consecutiva controllata da badge.

2.4 POLITICA DI CONTROLLO ACCESSI LOGICI

Il Responsabile Tecnico di Data Center, tramite i tool specializzati per la gestione delle utenze, provvede alle seguenti attività:

- Assegna ad ogni utente Var Group un codice identificativo (account) associato a una password riservata che verrà comunicata con processo certificato ISO 27001 solamente dall'incaricato stesso. La password dovrà essere sostituita dall'utente al primo utilizzo.
- Provvede a creare per quel codice identificativo un adeguato profilo di autorizzazione secondo le mansioni e le operazioni per cui l'utente è incaricato. L'assegnazione dei diritti e la condivisione di file, directory e dischi è limitata alle effettive necessità operative ed è attivata unicamente per il tempo strettamente indispensabile.
- Provvede a creare, per la stessa utenza, la possibilità di accedere tramite collegamento remoto (VPN). Tale accesso è regolato tramite l'aggiunta del doppio fattore di autenticazione su dispositivo mobile.
- Provvede ad istanziare il processo di enrollment sulla piattaforma centralizzata per la gestione del doppio fattore di autenticazione. Tale procedura consiste nel censire l'utente ed il relativo dispositivo mobile.

Sono inoltre rispettati i seguenti criteri:

- Il codice per l'identificazione non può essere assegnato ad altri incaricati, neppure in tempi diversi.
- Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai sistemi.
- Il sistema ricorda l'ultima password usata e non permette all'account di riusarle nel cambio successivo.

- É vietato l'utilizzo di user id di gruppo, cioè di una stessa utenza da parte di più dipendenti, dove i dispositivi lo consentano.
- Nei casi in cui i dispositivi non lo consentano, sono previsti user id univoci utilizzati da parte di utenti diversi; in tali casi è conservato l'elenco degli utenti ai quali sono stati comunicate le credenziali per l'accesso, indispensabili per l'attività operativa.
- Gli amministratori di sistema utilizzano credenziali di autenticazione nominali ad attribuzione univoca, anche nel tempo. In particolare, con specifico riferimento ai dipendenti di Var Group operanti in qualità di amministratori di sistema, è garantito il rispetto del Provvedimento del Garante della Privacy del 27 novembre 2008, così modificato in base al provvedimento del 25 giugno 2009. A tal fine Var Group provvede a identificare e a designare per iscritto gli amministratori di sistema, previa valutazione in ordine alle caratteristiche di capacità, affidabilità ed esperienza dei soggetti designati; il documento recante gli estremi identificativi delle persone fisiche preposte alla funzione di amministratori di sistema è conservato, per qualsiasi evenienza, ed è aggiornato ad ogni modifica. Inoltre, Var Group verifica, almeno annualmente, l'attività svolta dagli amministratori di sistema al fine di vagliare la sua rispondenza alle misure organizzative, tecniche e di sicurezza adottate rispetto alle normative vigenti. Al fine di tracciare le operazioni svolte dai propri amministratori di sistema, Var Group si avvale di un sistema di registrazione dei log che consente di monitorare le attività di accesso ai sistemi da parte degli stessi amministratori medesimi. Le registrazioni (access log) corrispondono alle caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste e comprendono i riferimenti allo "username" utilizzato, i riferimenti temporali e la descrizione dell'evento (log in e log out) che le ha generate. Si precisa, inoltre, che le registrazioni sono conservate per un tempo non inferiore a sei mesi.

Il Responsabile Tecnico di Data Center Var Group, avvalendosi dei suoi collaboratori, provvede a verificare che i diritti e i privilegi per gli accessi logici al personale interno corrispondano in ogni momento alle effettive necessità operative. Tali verifiche vengono condotte e registrate compilando apposita check list. Entro due settimane lavorative dalla cessazione del rapporto di lavoro la direzione del personale accerta che vengano eliminati account e privilegi assegnati alla persona uscente.

2.5 MISURE DI SICUREZZA GENERALI ADOTTATE

2.5.1 ACCESSO REMOTO E VPN

Ogni accesso remoto alla rete Var Group garantisce la stessa priorità e lo stesso livello di sicurezza di un utente on-site connesso. Si fa uso quindi di standard per la connessione remota progettati per ridurre al minimo l'esposizione potenziale ai danni che potrebbero derivare da un uso non autorizzato delle risorse di Var Group.

Accesso Remoto

- Sono implementate attività di controllo sull'accesso remoto tramite l'utilizzo di report giornalieri dal firewall che instaura la VPN e gestisce quindi l'autenticazione con doppio fattore
- Operatori di Var Group o utenti con privilegi di accesso remoto devono garantire che il computer da loro utilizzato sia di loro proprietà o di proprietà di Var Group, che non sia collegato a qualsiasi altra rete, allo stesso tempo, con eccezione delle reti personali/aziendali che sono sotto il controllo completo dell'utente.
- L'elenco dei software approvati per l'accesso remoto è essere reso solo a chi utilizzi accessi remoti
- La riconfigurazione delle apparecchiature di dispositivi "home user" allo scopo di "split-tunneling" o "dual homing" non è consentita.
- Tutti gli host che sono collegati alle reti Var Group con tecnologie di accesso remoto devono utilizzare versioni di software anti-virus con definizioni dei virus costantemente aggiornate.
- VPN

- Sono implementate attività di controllo sull'uso di VPN tramite l'autenticazione con doppio fattore di autenticazione e report giornalieri sull'utilizzo.
- In aggiunta alla password l'utente deve digitare il codice OTP (Token) disponibile sull'applicazione del dispositivo mobile in dotazione al dipendente.
- Quando l'utente è attivamente collegato alla rete aziendale, VPN costringe tutto il traffico da e verso il PC attraverso il tunnel VPN; tutto il restante traffico sarà rimosso.
- Dual (split) tunneling non è consentito; è consentita una sola connessione di rete.
- Il Gateway VPN è configurato e gestito da operatori qualificati di Var Group.

2.5.2 CONFIGURAZIONE FIREWALL

Regole di Firewall su router periferici

I Router di collegamento verso i carrier o verso gli operatori con i quali Var Group scambia connettività hanno delle regole di firewall utili a boccare quel traffico che, per la sua natura, non può arrivare dalla rete geografica o non può uscire verso la stessa. Un esempio di queste regole sono le access-list che impediscono il traffico nei due sensi delle classi IP IANA (quelle dedicate alle reti IP private).

Regole generali su Firewall condiviso

I server protetti dai Firewall Var Group condivisi la raggiungibilità degli stessi da IP e classi consentite e protette, in generale, da attacchi con tecnologie moderne.

Alcune regole possono essere anche sovrascritte da regole personalizzate, anche se le seguenti non sono discutibili:

- Controllo traffico reti IANA
- Controllo traffico sorgente
- Protezione da attacchi informatici basati sul volume di traffico e non sulla destinazione

Le regole personalizzate che auspicabilmente vengono concordate con il Cliente riguardano le aperture o le chiusure di porte specifiche TCP/UDP, aperture o chiusure di protocolli specifici, pubblicazione di servizi verso Internet in alcuni casi aperti solo o solo verso specifici indirizzi IP.

Policy di sicurezza su apparati di networking switch

Le porte degli switch sono tenute in shutdown se non in uso e vengono applicate le policy sulla segregazione delle VLAN.

Regole Firewall dedicati

In alcuni casi i Server sono protetti da firewall dedicati. Al momento dell'attivazione del servizio vengono configurate sugli apparati (fisici o virtuali) le policy richieste dal Cliente.

Tali Firewall possono essere:

- Gestiti dal Cliente: in questo caso le credenziali di amministratore vengono date da Var Group al Cliente dopo l'attivazione iniziale del servizio e il Cliente può modificarle in autonomia;

- Gestiti da personale Var Group: in questo caso le credenziali di amministratore del/dei firewall vengono conservate dal personale tecnico Var Group;
- Cogestiti: a seconda della richiesta del Cliente, una parte tra Var Group e il Cliente manterrà il controllo di amministratore sul/sui firewall, la restante parte avrà accesso al/ai firewall tramite la creazione di un secondo utente
- In ogni caso i server protetti da tali firewall sono sottoposti alle regole definite sui router periferici e sugli apparati di networking.

2.5.3 CONFIGURAZIONE ROUTER

Ogni router soddisfa le seguenti norme di configurazione e gestione:

- Gli account utente locali non sono configurati sul router. I router utilizzano Radius per tutte le autenticazioni degli utenti.
- La password di abilitazione sul router è conservata in una forma criptata.
- Il router ha settata la password di accesso in emergenza, password assegnata solo a personale qualificato e incaricato del settaggio e gestione dei router.
- Sono disabilitate le seguenti opzioni:
    - IP directed broadcasts
    - Pacchetti in ingresso al router indirizzati con indirizzi non validi come RFC1918
    - TCP small services
    - UDP small services
    - All source routing
    - All web services running on router
- Usare SNMP community string standardizzate e ad accesso ristretto (sola lettura).
- Ogni router è gestito con un punto di accesso logico e fisico sotto controllo.
- Ogni router riporta fisicamente la seguente dichiarazione: "È PROIBITO QUALSIASI L'ACCESSO NON AUTORIZZATO A QUESTO DISPOSITIVO DI RETE".
- È necessario disporre di un'esplicita autorizzazione da parte del Responsabile Tecnico di Data Center per accedere o configurare i router.
- Tutte le attività effettuate sui router sono registrate.
- Telnet non può mai essere utilizzato su qualsiasi rete per gestire un router a meno che non vi sia un tunnel sicuro a protezione dell'intero percorso di comunicazione. SSH è il protocollo di gestione preferita.
- Vengono utilizzate ACL, dove possibile, per bloccare il traffico indesiderato.

2.5.4 CONFIGURAZIONE SERVER

Tutti i server interni di Var Group sono sotto amministrazione di un gruppo operativo coordinato dal Responsabile Tecnico di Data Center, che stabilisce le linee guida di configurazione dei server.

Il gruppo operativo controlla il rispetto di configurazione. Le modifiche di configurazione per i server devono seguire le appropriate procedure di gestione dello stato di configurazione.

Inoltre, si devono rispettare le seguenti prescrizioni:

- Negli ambienti virtuali VMware non è attivata alcuna eventuale funzionalità dell'hypervisor che possa consentire una comunicazione tra le macchine virtuali differente da quella tramite rete.
- I servizi e le applicazioni che non sono utilizzati devono essere disabilitati, se possibile.
- L'accesso ai servizi deve essere registrato e/o protetto attraverso metodi di controllo accessi, come i wrapper TCP, se possibile.

- Sul sistema, quando possibile, sono installate le più recenti patch di sicurezza, con la sola eccezione rappresentata dal caso in cui l'applicazione vada ad interferire con requisiti tecnici o le richieste del Cliente.
- Sul sistema è installato un Anti Virus di ultima generazione con features aggiuntive legate agli aspetti comportamentali ed in grado di rispondere autonomamente alle minacce. Gli aggiornamenti sono automatici ed è integrato con la gestione degli eventi di sicurezza aziendali sul SIEM.
- Non sono configurate "trust relationship" tra i sistemi.
- Se una connessione "secure channel" è disponibile (e se ciò è tecnicamente possibile), l'accesso privilegiato deve essere eseguito "secure channel" (per esempio, connessioni di rete crittografate utilizzando SSH o IPSec).
- Tutti gli eventi relativi alla sicurezza nei sistemi sono registrati ed oggetto di audit periodico.

2.5.5 SICUREZZA DEI NOTEBOOK

I notebook utilizzati dal personale Var Group rispettano i seguenti criteri di sicurezza:

- protezione con Antimalware e EDR aggiornato quotidianamente e gestito tramite console centrale (monitorata H24 da SOC esterno);
- hard disk cifrato tramite Bitlocker;
- autenticazione al SO (Windows 10) tramite password con criteri di complessità e durata gestiti centralmente tramite Active Directory o Azure AD"sistema operativo e gli altri software applicativi risultano aggiornati tramite sistemi centralizzati (WSUS e EDR)

2.5.6 MONITORAGGIO E SICUREZZA COMPONENTI INFRASTRUTTURALI E RETE

Var Group garantisce che le impiantistiche delle componenti infrastrutturali di base, cioè quelle correlate alla fornitura continua di corrente elettrica e di condizionamento ambientale e delle risorse tecnologiche legate alla rete di trasmissione di dati, ai sistemi di erogazione dei servizi informatici relativi all'infrastruttura tecnologica dei Data Center di Var Group sono soggette a costante e continuo servizio di monitoraggio proattivo e di gestione dei processi da parte di un Network Operation Center 24x7.

Il monitoraggio delle componenti di facility viene effettuato tramite sensori collegati alle centraline di allarme integrate con un gruppo di manutentori certificati per la parte di competenza.

- Dal punto di vista della sicurezza Cyber Var Group ha predisposto un sistema di monitoraggio che interessa l'infrastruttura dei Data Center e gli applicativi sotto il proprio controllo. La gestione del sistema di monitoraggio è affidata ad un Security Operation Center operativo 24x7 ed è basata dalle seguenti componenti specifiche:
- SIEM (Strumento principale del SOC BU Digital Security);
- NAD (Network Anomaly Detection, integrato con il set dei monitoraggi sul SOC)
- EDR (Endpoint Protection and Response, integrato con la gestione degli eventi del SOC)

2.5.7 PROTEZIONE ANTI DDOS

A livello Data Center è presente una soluzione Anti DDOS (Distributed Deny Of Service) basata sulla soluzione di mercato Arbor di NETSCOUT. La soluzione consiste nella possibilità di intercettare anomalie sul volume del traffico e sulla quantità di pacchetti al secondo. Nel momento in cui queste soglie vengono superate il prodotto direziona il traffico verso il cloud di Arbor che elimina i pacchetti considerati malevoli e ritorna il traffico pulito verso il data center. Il servizio è un default per tutte le classi IP di Var Group. Il cliente ha la possibilità di acquistare un servizio AntiDDOS personalizzato per le proprie esigenze

2.5.8 VULNERABILITY ASSESSMENT & PENETRATION TEST

Var Group effettua periodici Vulnerability Assessment sulle infrastrutture di Data Center, i server, gli apparati di rete ed i sistemi, compresa la piattaforma VAR HUB, che sono sotto il proprio controllo e vengono utilizzati per l'erogazione dei servizi cloud. Inoltre vengono effettuati VA ogni qualvolta una nuova risorsa venga pubblicata e ogni qualvolta venga individuato un evento anomalo al fine di verificare che l'infrastruttura/soluzione/servizio rilasciata a ciascun Cliente in ambito cloud non abbia:

- Vulnerabilità tali da compromettere la propria sicurezza e quella del Data Center
- Vulnerabilità non conosciute dal personale di riferimento
- Vulnerabilità non gestite

Ulteriori Vulnerability Assessment possono essere successivamente effettuati in base a quanto concordato con il Cliente.

Nel caso durante le attività di Vulnerability Assessment siano state riscontrate delle vulnerabilità sfruttabili, Responsabile Tecnico di Data Center Var Group può prevedere l'esecuzione di Penetration Test sui target individuati. Le attività previste dal Penetration Test per testare le risorse che risultano esposte a possibili attacchi che ne compromettano il livello di sicurezza devono conseguire uno dei seguenti obiettivi:

- Verificare che la vulnerabilità non sia un falso positivo
- Verificare quanto possa essere compromesso il sistema in caso di sfruttamento della vulnerabilità
- trasmettere i risultati al Data Center Security Team

Una vulnerabilità è definita gestita quando:

- Per essa si è definito un piano di remediation mediante patching, update, upgrade o modifiche alla configurazione;
- La vulnerabilità è conosciuta dal personale per essa non può essere definito/applicato un piano di remediation, ma è funzionale all'erogazione di un servizio/applicazione. Vengono comunque attuate misure di attenuazione mediante altri dispositivi/policy di sicurezza (firewall, ids, logging).

In entrambi i casi viene documentato o il piano di remediation o quello di gestione della vulnerabilità.

NOTA: Si specifica che tutti i dispositivi aziendali sono sincronizzati con il dispositivo NTP interno (ridondato), che utilizza un NTP server Stratum 1.

2.6 MISURE DI SICUREZZA ADOTTATE PER LO SPECIFICO SERVIZIO

2.6.1 VIRTUAL PRIVATE SERVER

Il servizio di Virtual Private Server consiste nell'erogazione di server virtuali da una piattaforma di virtualizzazione condivisa. Le Virtual Machine attivate da Var Group per tale servizio possono essere:

- Protette da firewall statefull inspection condiviso (*rif. Paragrafo 2.5.2*)
- Protette da firewall virtuale dedicato a gestione di Var Group e/o del Cliente (*rif. Paragrafo 2.5.2*), ove contrattualizzato

A bordo macchina il Cliente può inoltre configurare in autonomia le regole del firewall presente sul server stesso (Windows Firewall o IP Tables a seconda del S.O. utilizzato).

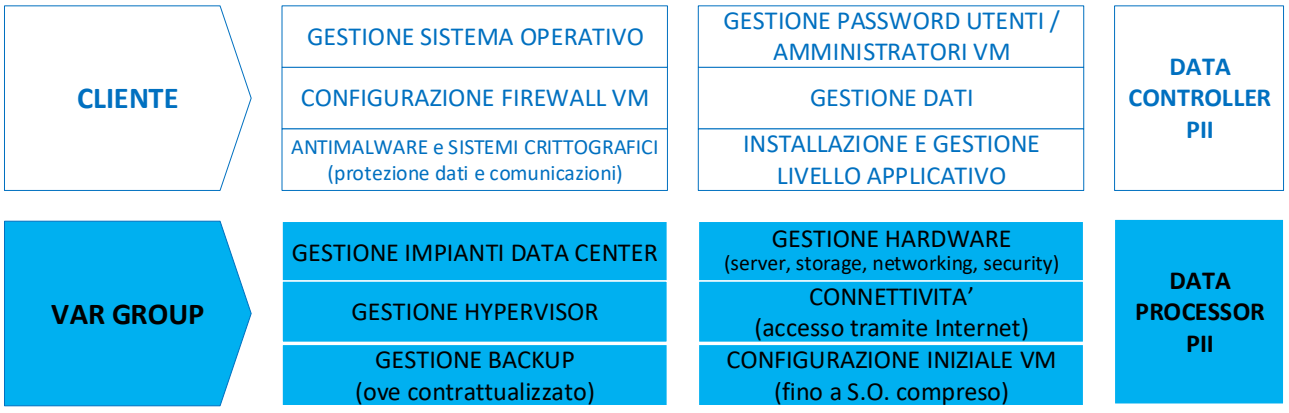
Le password di amministratore delle VM vengono consegnate da Var Group al Cliente al momento dell'attivazione del servizio; il Cliente sarà obbligato a modificare le password al primo utilizzo in modo da riservarsi l'accesso amministrativo.

Una volta completata la configurazione iniziale delle VM, Var Group consegna al Cliente il report relativo al Vulnerability Assessment condotto sulle copie master delle VM per attivate.

Var Group potrà eventualmente condurre, come servizio aggiuntivo, Vulnerability Assessment al termine dell'installazione degli applicativi sulle VM; sempre come servizio opzionale aggiuntivo, potranno inoltre essere schedulati Vulnerability Assessment periodici per valutare lo status di sicurezza delle VM utilizzate dal Cliente.

Infine si segnala che nel pacchetto base del servizio non è incluso il servizio di Backup o salvataggio di copia dei dati del Cliente. Pertanto, se il servizio di backup gestito non viene appositamente contrattualizzato ed attivato, il Cliente prende atto ed accetta che in caso di guasti o malfunzionamenti è possibile che si verifichi la perdita, parziale e/o totale, dei propri dati; al fine di scongiurare tale evenienza, sarà responsabilità del Cliente, a propria cura e spese, provvedere ad eseguire il backup e la copia di qualsiasi proprio dato.

RUOLI E RESPONSABILITA' CONDIVISI per la sicurezza delle informazioni ed il trattamento dei dati personali:



2.6.2 VIRTUAL DATA CENTER

Il servizio di Virtual Data Center mette a disposizione un pool di risorse organizzato per utilizzi di tipo business. Il Virtual Data Center utilizza la tecnologia VMware vCloud, che offre la massima compatibilità con gli ambienti di virtualizzazione di VMware.

Il servizio di Virtual Data Center comprende sempre risorse computazionali (CPU e RAM), spazio disco, Indirizzi IP pubblici, banda Internet, secondo i dimensionamenti e le quantità contrattualizzate. Sono inoltre inclusi un servizio di firewall virtuale dedicato (VMware vShield Edge) ed un servizio di back-up "full-VM".

L'infrastruttura da cui viene erogato il servizio di Virtual Data Center è protetta da firewall gestiti da Var Group per il blocco del traffico malevolo.

Ogni singolo Cliente può poi configurare in autonomia a protezione delle proprie risorse il firewall VMware vShield Edge incluso nel servizio. Il Cliente può eventualmente richiedere l'integrazione del servizio con l'installazione di firewall fisici dedicati.

Il Cliente è inoltre completamente autonomo nelle operazioni di creazione, configurazione, attivazione, accensione, spegnimento, eliminazione delle singole Virtual Machine all'interno del pool di risorse contrattualizzato. Var Group non ha mai visibilità delle password di amministratore per i singoli server virtuali attivati dal Cliente.

La soluzione Virtual Data Center comprende un servizio di backup "full-VM" con la seguente politica: un salvataggio "full-VM" alla settimana con archiviazione di due punti di ripristino.

Il backup di tipo "full-VM" sfrutta le funzionalità dei sistemi di virtualizzazione che consentono di ottenere un'immagine delle macchine virtuali. Questa immagine è molto utile per il ripristino completo della VM stessa quando non si è più in grado di utilizzarla nella consueta modalità per varie cause (ad esempio crash, file system corrotto, errore umano).

Si segnala che questo tipo di salvataggio è tipicamente "Crash Consistent" e solo in pochi casi garantisce anche l'integrità referenziale dei dati, tipica dei database.

RUOLI E RESPONSABILITA' CONDIVISI per la sicurezza delle informazioni ed il trattamento dei dati personali:

CLIENTE	CREAZIONE E GESTIONE VM	GESTIONE PASSWORD UTENTI / AMMINISTRATORI VM	**DATA CONTROLLER PII**
	GESTIONE FIREWALL vShield	GESTIONE DATI	
	ANTIMALWARE e SISTEMI CRITTOGRAFICI (protezione dati e comunicazioni)	INSTALLAZIONE E GESTIONE LIVELLO APPLICATIVO	
VAR GROUP	GESTIONE IMPIANTI DATA CENTER	GESTIONE HARDWARE (server, storage, networking, security)	**DATA PROCESSOR PII**
	GESTIONE HYPERVISOR	CONNETTIVITA' (accesso tramite Internet)	
	GESTIONE BACKUP «FULL-VM»		

2.6.3 SERVIZIO BACKUP APPLICATIVO (AMBIENTI VMWARE E MS HYPER-V)

Ove il Cliente contrattualizzi il servizio di backup, Var Group si impegna a:

- Identificare la metodologia di backup ottimale allo svolgimento del programma
- Custodire le politiche, i riferimenti tecnici e di contatto delle persone coinvolte
- Monitorare l'andamento del piano dei salvataggi

Var Group garantisce al Cliente di sottoporre a servizio tutti gli oggetti inizialmente concordati con le relative politiche di frequenza e retention. Nell'ottica di fornire un servizio di qualità, sarà possibile, secondo necessità, richiedere una modifica degli oggetti, della frequenza e della retention degli oggetti sottoposti al servizio anche successivamente alla prima attivazione. Per tutti gli oggetti non dichiarati invece, Var Group è manlevata da ogni responsabilità per i pregiudizi che il Cliente dovesse subire (es. perdita di informazioni e dati personali) come conseguenza della mancata sottoposizione al servizio di determinati oggetti per causa imputabile al Cliente o scelta da parte del medesimo. Sugli oggetti non sottoposti al servizio per causa imputabile al Cliente o per scelta del medesimo, pertanto, Var Group non garantisce alcun livello di servizio.

La parte sottoscrivente ha la facoltà di poter verificarne la funzionalità del servizio di backup, andando a consultare il file di LOG del/degli agenti di backup locali in qualsiasi momento. Su richiesta specifica è possibile fornire un'apposita credenziale di logon che permetta la consultazione diretta di quello che è ripristinabile dal "sistema storage". È possibile anche inviare una e-mail con l'esito del/i job di backup.

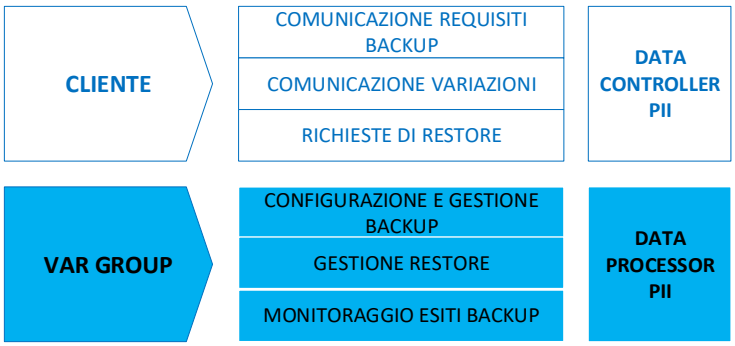
Var Group si impegna ad avvisare il Cliente al raggiungimento di soglie concordate di occupazione dello spazio disco delle Virtual Machine attivate. A seguito di questa comunicazione, il Cliente viene invitato ad effettuare tempestivi accorgimenti, con la liberazione di spazio disco tramite la cancellazione di file o l'acquisto di spazio disco aggiuntivo.

Var Group controlla quotidianamente l'esito dei salvataggi: verrà analizzata la causa di eventuali fallimenti e deciso quali attività di remediation intraprendere.

È responsabilità del Cliente comunicare eventuali modifiche o importanti aggiornamenti nella configurazione dei propri sistemi. In assenza di integrazioni o variazioni senza debita comunicazione, Var Group non garantisce sulla qualità del servizio di backup erogato, ritenendo l'erogazione del tutto consona alle aspettative di salvaguardia del Cliente come da indicazioni riportate al momento dell'attivazione del servizio.

Trascorsi 30 giorni dalla data di scadenza del contratto, o nel caso di dismissione per altri motivi, l'azienda si impegna ad eliminare ogni copia parziale, totale, temporanea o definitiva dei dati sottoposti a backup.

RUOLI E RESPONSABILITA' CONDIVISI per la sicurezza delle informazioni ed il trattamento dei dati personali:



2.6.4 PARTIZIONI IBM POWER i IN CLOUD

Il servizio Power i in cloud consiste nell'erogazione di una partizione virtuale (LPAR) Power i, realizzata tramite l'apposita piattaforma IBM di virtualizzazione dinamica PowerVM VIOS su macchine fisiche condivise collocate presso il Data Center Var Group. Le LPAR attivate da Var Group possono essere:

- Protette da firewall statefull inspection condiviso (*rif. Paragrafo 2.5.2*)
- Protette da firewall dedicato a gestione di Var Group e/o del Cliente (*rif. Paragrafo 2.5.2*), ove contrattualizzato

Nelle attività di configurazione iniziale del servizio offerto, sono incluse e quindi a carico di Var Group le seguenti attività:

- Installazione S.O., patch PTF e software aggiuntivi IBM contrattualizzati
- Configurazione rete (IP, gateway)
- Configurazione backup (effettuato tramite strumento BRMS) secondo le policy contrattualizzate; il backup, di default, include tutto lo spazio storage, i dati utente e di sicurezza.

Terminate le attività sopra elencate, il reparto tecnico Var Group consegna le credenziali di amministrazione della partizione al Cliente; il Cliente da questo momento è autonomo nella creazione dei vari utenti che dovranno avere accesso al servizio e nella configurazione dei permessi che avrà ciascuno di essi.

Si segnala che Var Group, di default, al momento della consegna delle credenziali di amministrazione lascia attivo sulla LPAR un secondo utente per l'accesso alla partizione per manutenzione ed assistenza.

Il Cliente può decidere in ogni momento di disabilitare questo utente; in questo caso il Cliente abiliterà l'utente o ne configurerà uno nuovo ogni qualvolta si rendesse necessario un intervento di assistenza da parte di Var Group (ad es. per un controllo sui backup). In questo caso, inoltre, la gestione di aggiornamenti e patch di sistema, solitamente a carico di Var Group ed inclusa nel servizio, sarà invece responsabilità del Cliente.

RUOLI E RESPONSABILITA' CONDIVISI per la sicurezza delle informazioni ed il trattamento dei dati personali:

CLIENTE	GESTIONE SISTEMA OPERATIVO	GESTIONE PASSWORD UTENTI / AMMINISTRATORI VM	**DATA CONTROLLER PII**
	CONFIGURAZIONE FIREWALL VM	GESTIONE DATI	
	ANTIMALWARE e SISTEMI CRITTOGRAFICI (protezione dati e comunicazioni)	INSTALLAZIONE E GESTIONE LIVELLO APPLICATIVO	
VAR GROUP	GESTIONE IMPIANTI DATA CENTER	GESTIONE HARDWARE (server, storage, networking, security)	**DATA PROCESSOR PII**
	GESTIONE HYPERVISOR	CONNETTIVITA' (accesso tramite Internet)	
	GESTIONE BACKUP (ove contrattualizzato)	INSTALLAZIONE S.O. E PACCHETTI IBM	

2.6.5 HOSTING SITI WEB

Questo servizio consiste nella fornitura di uno spazio per l'hosting e la gestione del sito web del Cliente, erogato da piattaforma condivisa ed ottimizzata per i seguenti applicativi: Joomla, Magento, Wordpress, Moodle, DNN – DotNetNuke.

La piattaforma utilizzata per l'erogazione del servizio è:

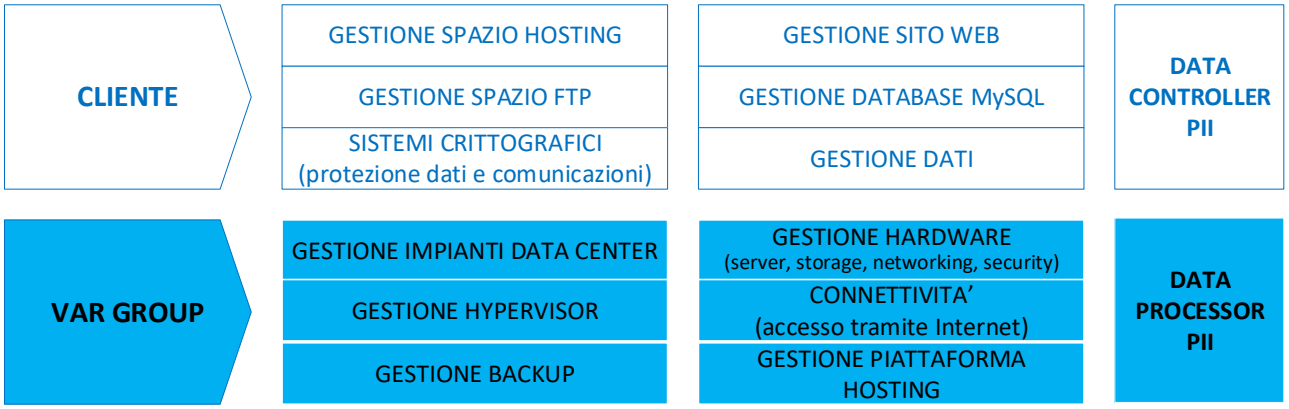
- Protetta da firewall statefull inspection condivisi (rif. Paragrafo 2.5.2)
- Protetta da WAF (Web Application Firewall) per la protezione dagli attacchi informatici più noti

Al momento dell'attivazione del servizio, il reparto tecnico Var Group procede alla creazione dello spazio di hosting e dei relativi spazi FTP e database MySQL.

Le credenziali dello spazio FTP e del database vengono consegnate che potrà modificarle in autonomia in ogni momento.

Var Group rimane amministratore di sistema della piattaforma di hosting.

RUOLI E RESPONSABILITA' CONDIVISI per la sicurezza delle informazioni ed il trattamento dei dati personali:



2.6.6 POSTA ELETTRONICA GESTITA - ZIMBRA

La sicurezza relativa al servizio di posta elettronica Zimbra è garantita mediante applicazione di politiche restrittive in relazione all'accesso da parte del personale aziendale alle virtual machine Zimbra (autenticazione LDAP), mediante attività di backup, svolta 4 volte a settimana (con archiviazione di 4 restore point), cui è soggetta la configurazione delle virtual machine. La piattaforma Zimbra è inoltre protetta da firewall statefull inspection che consente, in considerazione di esigenze specifiche, l'apertura e chiusura di porte TCP/IP.

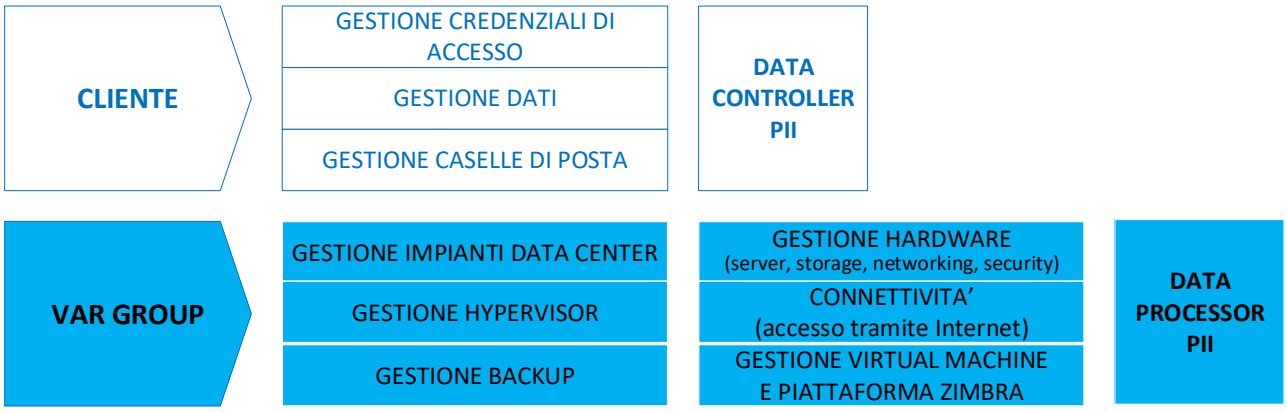
Qualora il cliente possegga un indirizzo IP statico, è fornito un pannello di gestione del dominio e delle singole caselle e il firewall consente l'accesso protetto dal solo IP cliente alla console amministrativa.

I servizi nativi di antivirus e antispam possono essere integrati con servizi di antivirus e antispam esterni

Vengono offerti i servizi IMAPS, POP3S, SMTPS, SMTP, HTTPS

È compreso un servizio di backup nativo delle caselle mail, con salvataggio dei dati giornaliero incrementale relativo agli ultimi 7 giorni e salvataggio full settimanale, con archiviazione delle ultime 4 settimane

RUOLI E RESPONSABILITA' CONDIVISI per la sicurezza delle informazioni ed il trattamento dei dati personali:



3 SERVIZIO SaaS - VAR HUB

3.1 VAR HUB - AMBITO E RUOLI

VAR HUB è il servizio integrato di fatturazione elettronica e conservazione sostitutiva progettato e implementato da Var Group sui propri ambienti cloud ed erogato dai propri Data Center.

A differenza dei servizi **IaaS** (*Infrastructure-as-a-Service*) descritti nel capitolo precedente, VAR HUB rappresenta una soluzione **SaaS** (*Software-as-a-Service*). In questo caso, quindi, la gestione di Var Group non si limita all'infrastruttura fisica e alla piattaforma di virtualizzazione, ma si estende anche ai server virtuali, ai relativi Sistemi Operativi, ed alle applicazioni installate. Il Cliente accederà al servizio autenticandosi su portale web tramite il quale potrà inviare, ricevere ed archiviare fatture in formato elettronico tramite l'intermediario fiscale Var Group.

Il Cliente resta comunque Titolare del trattamento (*Data Controller*) e Var Group agirà di conseguenza in qualità di **Data Processor** (*Responsabile del trattamento*), per tale intendendosi, ai sensi dell'art. 4, par. 1, punto 8 del Regolamento UE 2016/679, "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

Ove non diversamente indicato, le condizioni generali di servizio e le responsabilità di Var Group descritte nel presente documento sono da ritenersi pertanto valide anche per il servizio VAR HUB.

Essendo tuttavia maggiormente esteso l'ambito di responsabilità tecnica di Var Group, le misure di sicurezza standard adottate per lo specifico servizio VAR HUB sono più avanzate rispetto a quelle descritte al paragrafo 2.6 del presente documento e l'autonomia concessa al Cliente per la personalizzazione di tali misure risulta ridotta.

Vengono riportate a seguire le condizioni generali di servizio e le misure di sicurezza adottate specificatamente per la piattaforma SaaS VAR HUB; per i Clienti che non reputano sufficienti i requisiti decritti di seguito, Var Group può progettare e implementare una soluzione di fatturazione elettronica e conservazione sostitutiva basata su infrastruttura dedicata. In questo scenario, le misure di sicurezza e le condizioni del trattamento dei dati verranno discusse e condivise con il cliente caso per caso.

3.2 VAR HUB - GESTIONE E CANCELLAZIONE DEI DATI

Var Group si impegna a garantire che, per tutta la durata contrattuale, sia possibile per il Cliente procedere in autonomia al download dei documenti non ancora conservati e alla creazione (e al relativo download) dell'immagine ISO a norma per i documenti già in conservazione.

Var Group si impegna in caso di cessazione, per qualsiasi motivo, dei rapporti con il Cliente a mettere a disposizione, fatti salvi gli obblighi derivanti dallo scarto dei documenti conservati nel rispetto del D.P.C.M. del 3 dicembre 2013, la documentazione generata, archiviata e conservata per mezzo degli strumenti messi a disposizione del servizio VAR HUB e di ogni altra riconducibile allo stesso, in qualunque formato disponibile, in tempo utile (e comunque compatibilmente con gli obblighi ancora pendenti in capo a Var Group anche in ragione delle deleghe e degli incarichi ricevuti) per il Cliente ad evitare indebite interruzioni delle attività di rilievo e altresì al fine di trasferire la stessa ad eventuale diverso fornitore o comunque di trasferirla direttamente a questo mediante canali sicuri e previa autorizzazione del Cliente.

In alternativa, fatti salvi gli obblighi derivanti dallo scarto dei documenti conservati ai sensi del D.P.C.M. del 3 dicembre 2013, Var Group si impegna a cancellare o rendere inintelligibile la documentazione generata, archiviata e conservata per mezzo degli strumenti messi a disposizione del servizio VAR HUB, allorché il Cliente lo autorizzi in tal senso manlevandolo da ogni responsabilità al riguardo. In ogni caso a conclusione delle operazioni descritte, Var

Group non potrà essere ritenuta responsabile in ordine all'adempimento di obblighi ulteriori, salvo quelli che lo impegnano alla riservatezza e nei limiti per essi stabiliti.

Alla cessazione del servizio, Var Group, dopo apposita comunicazione, metterà a disposizione del Cliente la possibilità di scaricare i documenti non ancora andati in conservazione e la possibilità di generare e scaricare, in autonomia tramite il portale, le immagini ISO autoconsultanti dei lotti conservati senza nessun ulteriore addebito. Il Cliente avrà 60 giorni di tempo, a partire dalla data della suddetta comunicazione, per collegarsi al portale, scaricare i documenti e/o generare e scaricare le immagini ISO dei lotti.

Qualora il Cliente voglia commissionare a Var Group la generazione delle immagini ISO autoconsultanti dei lotti conservati, dovrà comunicarlo con apposita richiesta a mezzo PEC; tale operazione comporterà dei costi addizionali a carico del Cliente, così come da listino. Il Cliente avrà 60 giorni di tempo, a partire dalla data di comunicazione dell'avvenuta conclusione della procedura di preparazione dati, per effettuare il download.

In ogni caso trascorsi i 60 giorni di cui sopra i documenti, le immagini e i relativi dati verranno eliminati e non saranno più accessibili né dal portale né in altro modo.

Scaduto il periodo di conservazione, concordato contrattualmente tra il Cliente e Var Group, viene avviata la procedura di Scarto concordata, con la produzione del Pacchetti di Scarto e la verbalizzazione dello scarto e della chiusura del servizio.

Prima dell'avvio dello scarto e della procedura di chiusura del Servizio, che si conclude con una verbalizzazione dell'attività, viene comunicato al Cliente l'avvio dello scarto entro 30 gg al fine di fornirgli un periodo transitorio per richiedere formalmente l'estensione (prolungamento) del periodo di conservazione. Inoltre come da disposizioni del codice dei beni culturali (D. Lgs. 22 gennaio 2004, n.42) nel caso di enti pubblici o privati dichiarati di notevole interesse storico, per effettuare lo scarto verrà richiesta l'autorizzazione preventiva alla Soprintendenza Archivistica da parte del Produttore.

3.3 VAR HUB - MISURE DI SICUREZZA ADOTTATE

Le VM tramite cui viene erogato il servizio integrato di fatturazione elettronica e conservazione sostitutiva denominato VAR HUB sono ospitate su cluster VMware in configurazione di alta affidabilità. Tutti i componenti dell'infrastruttura sono completamente gestiti da Var Group, compreso il firewall WAF (Web Application Firewall) posto a protezione della piattaforma VAR HUB.

VAR HUB è una soluzione multi-tenant; ciò significa che diversi Clienti condividono le risorse virtuali, accedendo però ad ambienti logicamente separati. Vengono applicate diverse misure di sicurezza, policy e regole per evitare che un Cliente abbia accesso ai dati degli altri Clienti con cui condivide la piattaforma virtuale.

Tutte le VM dell'infrastruttura VAR HUB sono sottoposte a backup, che viene effettuato quotidianamente e prevede l'archiviazione di 7 punti di ripristino, quindi con una retention pari ad una settimana completa. Tale backup consiste in due step differenti:

- Backup "full-VM" delle VM;
- Backup applicativo del Database.

La connessione tra il sito del Cliente e VAR HUB è resa sicura da un certificato SSL valido, emesso da una CA (Certification Authority) pubblica, che salvaguarda i dati inviati e ricevuti da letture o modifiche malevole.

Sull'ambiente virtuale da cui viene erogata la soluzione VAR HUB Var Group ha attivato un servizio di replica e D.R. su un sito secondario. Tale soluzione di D.R. prevede l'uso di un software specifico per la replica delle VM tra il sito primario ed il sito secondario (rispettivamente situati a Milano ed Empoli). Questa tecnologia di replica, che opera a livello dell'hypervisor, permette la replica delle applicazioni e dei dati più critici con livelli di RTO (Recovery Time Objective) e RPO (Recovery Point Objective) minimi.

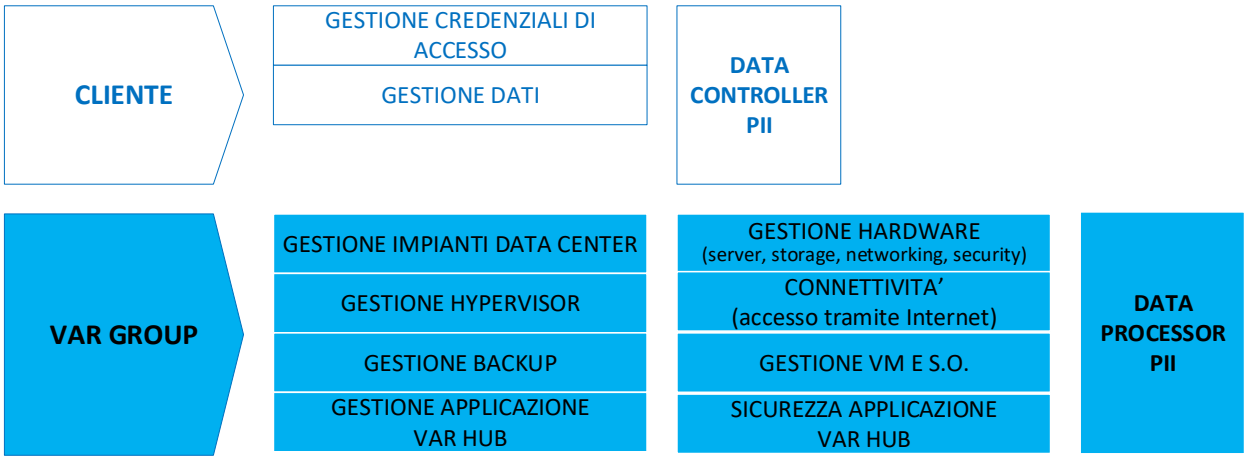
Al fine di garantire sempre l'efficienza della soluzione di D.R. Var Group ha redatto un Disaster Recovery Plan (D.R.P.), un manuale contenete le operazioni da seguire nel caso in cui si renda necessario il ripristino del servizio sul sito secondario. Tale manuale viene controllato e mantenuto aggiornato tramite l'organizzazione di periodici Disaster Recovery Test (D.R.T.), simulazioni di ripristino, che, se non si verificano eventi eccezionali, vengono effettuati da Var Group almeno ogni dodici mesi.

Al momento dell'attivazione di VAR HUB, le credenziali di accesso vengono inviate al Cliente. Il sistema obbligherà il cliente a modificare la password di accesso alla soluzione dopo il primo login. Le credenziali di accesso possono essere resettate remotamente da Var Group in ogni momento. Se un Cliente sospetta una violazione, o tali credenziali vengono compromesse, il Cliente può richiedere a Var Group il reset della password. Il sistema invierà al Cliente la nuova password e, anche in questo sarò, verrà obbligatoriamente richiesta la modifica della stessa dopo il primo accesso.

L'attivazione standard di Var Group prevede la creazione di un singolo utente per ciascun Cliente; quindi, al momento dell'attivazione, ogni Cliente riceverà un solo username d'accesso e la relativa password. Come servizio opzionale aggiuntivo (a pagamento), Var Group può attivare utenti addizionali per il Cliente, consentendo quindi accessi multipli alla soluzione. Anche per gli utenti aggiuntivi sarà obbligatorio modificare la password fornita da Var Group dopo il primo accesso.

Le attività possibili attraverso la piattaforma VAR HUB sono descritte nel Manuale Operativo consegnato al momento della contrattualizzazione del servizio ed esse rimangono altresì tracciate (nel c.d. registro di log) ai fini del loro corretto svolgimento e della loro riconducibilità ai soggetti autorizzati all'accesso, anche in caso delle ordinarie e/o straordinarie attività tecniche di manutenzione della piattaforma e dell'applicativo da parte di Var Group.

RUOLI E RESPONSABILITA' CONDIVISI per la sicurezza delle informazioni ed il trattamento dei dati personali:



4 CONTATTI VAR GROUP

Viene riportato a seguire un elenco di riferimenti che i Clienti possono utilizzare per contattare Var Group riguardo ai temi di protezione dei dati o di sicurezza relativa al servizio contrattualizzato.

Funzione	Contatti
Informazioni Generali	Numero Verde: 800 646 543 Tel: 0571 9988 Fax 0571 998062 Email: info@vargroup.it
Ufficio Quality & Compliance	Email: qualityecompliance@vargroup.it
Information Security Office Var Group	Email: cybersecurityvg@vargroup.it
Ufficio Digital Law & Data Protection	Email: Digitallaw&dataprotection@vargroup.it
Sicurezza Data Center Var Group	Email: security@leonet.it
Responsabile Servizio VAR HUB	Email: m.bargellini@vargroup.it
Responsabile Tecnico Data Center	Tel: 0571 9988 051 Email: f.barsotti@vargroup.it
Help Desk Servizi Cloud	Numero Verde: 800 400 000 Email: helpdeskmycloud@vargroup.it
Data Protection Officer	Email: dpo@sesa.it

5 CRONOLOGIA DELLE REVISIONI

Data	Rev. Num.	Descrizione
25/05/2018	01	Prima stesura
10/10/2018	02	Correzione ed aggiornamento misure di sicurezza
20/11/2018	03	Aggiunto capitolo relativo al servizio VAR HUB
08/01/2019	04	Indicazione fornitura report VA sulle copie master delle VM Private Server
31/05/2019	05	Aggiornamento campo applicazione ISO/IEC 27001
11/07/2019	06	Correzione contatti di riferimento Var Group
31/07/2019	07	Inserimento definizione ruoli condivisi
08/10/2019	08	Correzione ed aggiornamento misure di sicurezza
02/03/2020	09	Inserimento indicazione NTP, aggiornamento contatti finali
01/03/2022	10	Aggiornamento campo applicazione