Autore	Ufficio Compliance
Approvazione	Direzione

Versione Revisione

Versione	Autore	Consultazione DPO	Data emissione	Motivo della revisione
0.0	Ufficio Compliance	15/06/2026	15/06/2026	Prima emissione

PARERE DPO
OK.

Bisy Srl
Via Delfini, 26, 41123 Modena (MO)
Tel 059 867 6227 | Fax 059 867 6227
info@bisy.it | **www.bisy.it**

R.I. / C.F. e P.IVA n. 03441810367
R.E.A n. MO-388045
Capitale Sociale € 25.000 i.v.

ZENERGY UTILITY

RESPONSABILE DEL TRATTAMENTO					
Denominazione	**BISY S.r.l.**				
Partita Iva	03441810367				
Indirizzo	Via A. Delfini n. 26				
Città	Modena	**Cap**	41123	**PV**	MO
Legale Rappresentante	Federico Stradi				

INCARICATI DEL TRATTAMENTO
Sviluppatori, Delivery, Direzione ed Amministrazione

DATI DI CONTATTO			
Responsabile del trattamento	BISY s.r.l.	amministrazione@bisy.it	
Responsabile protezione dati (DPO)	Z Holding Spa	ufficio.privacy@zucchetti.it	

DESCRIZIONE

La piattaforma software ZENERGY UTILITY è in grado di acquisire fatture energetiche direttamente dal PDF del fornitore, di estrarne la totalità dei contenuti in modo automatico, di controllarne la validità ed analizzarne i dati in esse contenuti.

È formata da diversi Moduli operativi:

- "*Importazione*": prevede la possibilità di importare le fatture da diversi formati (PDF, XML-SDI, da tracciato xls e da tracciato strutturato;
- "*Controllo*": permette di controllare la correttezza delle fatture, fornendo anche report a supporto di reclami;
- "*Analisi*": fornisce dashboard e report di analisi; alert relativi a buchi di fatturazione o personalizzabili; permette la creazione di indici di performance personalizzati, nonché permette di fare una previsione dei costi mediante simulazione;
- "*Automazione*": permette una serie di attività automatiche nonché la possibilità di integrazioni con altri applicativi sw aziendali mediante API Restful;
- *"App"*: con cui si possono inviare i dati di autolettura alla piattaforma;
- "*Supporto*": per creare ticket di assistenza.

Questi moduli sono o meno presenti in base al livello di servizio contrattualizzato.
La piattaforma è fornita solo in cloud.

FINALITA' DEL TRATTAMENTO

La finalità della piattaforma è quella di analizzare le bollette di energia elettrica, gas e acqua, verificarne la correttezza e la registrazione automatica di tutte le informazioni riguardanti le utilities aziendali.
La finalità del trattamento è quella di erogare i servizi di formazione, assistenza e manutenzione al Titolare (che può essere tanto un concessionario quanto una Società di consulenza)

CATEGORIA INTERESSATI
Clienti, Dipendenti dei clienti.
CATEGORIE DI DATI PERSONALI
Anagrafiche di contatto dei dipendenti che accedono alla piattaforma, nonché credenziali dei clienti per accedere al portale del fornitore di servizi.
CATEGORIA DI DESTINATARI A CUI I DATI POTRANNO ESSERE COMUNICATI
Zucchetti Spa, DC service provider Società del Gruppo Zucchetti (per assistenza se contrattualizzate)
TRASFERIMENTO DATI ALL'ESTERO
No. I dati sono ubicati in Italia.
TERMINI PER LA CANCELLAZIONE DEI DATI
Alla conclusione del rapporto col cliente, su richiesta dello stesso, saranno consegnati copia dei dati e della struttura logica (ossia l'organizzazione delle informazioni) realizzati per l'esecuzione del servizio commissionato. Su richiesta del cliente possono essere eliminati o anonimizzati, entro 90 giorni dalla chiusura del contratto. I backup sono conservati per 90 giorni, quindi, gli stessi dati rimarranno nei backup per un massimo di 90 giorni dall'avvenuta cancellazione.

DESCRIZIONE GENERALE DELLE MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

1. MISURE DI SICUREZZA IMPLEMENTATE NEI SOFTWARE

Le misure di sicurezza configurabili nel sistema applicativo sono:

- ***Gestione credenziali di accesso***

- L'accesso al sistema avviene tramite username o indirizzo e-mail univoco e corrispondente password. Le utenze di Bisy sono o di tipo amministrativo e le stesse potranno, creare/modificare/cancellare le utenze e variare i privilegi di ciascun account.
- Le utenze potranno sempre essere disattivate su richiesta, sia dagli utenti admin che dal servizio di helpdesk.
- Ciascun utente può resettare in autonomia la sua password, tramite l'invio di un link temporaneo al proprio indirizzo e-mail.
- Ripetuti errori di accesso causeranno un blocco temporaneo dell'indirizzo ip dal quale gli stessi provengono, per evitare tentativi di brute forcing della password.
- È possibile configurare l'accesso al sistema tramite protocollo standard OAUTH 2.0, sfruttando così un eventuale sistema di autenticazione già in uso al Cliente senza necessità di creare nuove credenziali e rispettando tutti i criteri di complessità già configurati dal Cliente stesso.

- ***Minimizzazione:***

- Profili di autorizzazione: il Titolare, mediante l'intervento del Responsabile, può configurare l'accesso ai dati personali trattati nel sistema a seconda delle attività svolte dagli utenti.

- ***Identificazione di chi ha trattato i dati:***

- Strumenti di log: Tutte le attività eseguite sulla piattaforma tanto dal Cliente/Titolare quanto dal Responsabile e dagli utenti del personale di assistenza sono loggate. I log sono trasmessi e conservati in una piattaforma dedicata per 90 giorni.
- Presenza di utenze di servizio per personale di assistenza: Coloro che eseguono assistenza e manutenzione sulla piattaforma hanno utenze nominali.

- ***Tecniche di crittografia:***

- Crittografia delle password: per le password viene registrato un hash delle password con l'algoritmo *PBKDF2* aggiungendo un "salt" di applicazione ed un "salt" di utente. Le credenziali di servizi esterni sono memorizzate cifrate tramite crittografia simmetrica.
- Crittografia file DMS: tutti i documenti generati dalle applicazioni e conservati nel DMS sono crittografati.

- ***Privacy by default***

- Attivazione profilo utente: gli utenti nel portale sono attivati secondo una logica di non assegnare alcun profilo autorizzativo sui dati trattati. Sarà il Titolare in autonomia a scegliere

la profilazione utente idonea e ad attribuire le autorizzazioni in funzione dell'area omogenea di cui fa parte l'utente o del profilo di autorizzazione individuale.

- ***Diritti degli interessati***:

- Diritti degli interessati: per garantire agli interessati il diritto all'oblio, è sufficiente che inviino una richiesta al Titolare che richiederà a Bisy la cancellazione dei dati dell'utente, che avverrà entro 90 giorni.
- Per garantire il diritto dell'interessato di avere informazione su quali dati sono trattati dal Titolare e alla portabilità dei suoi dati, è possibile richiedere a Bisy l'esportazione dei log delle attività dell'utente in formato strutturato CSV.
- Il Cliente può richiedere di anonimizzare i dati personali degli interessati con apposite query. Potranno essere anonimizzati i soli dati correnti, mentre le informazioni nei log potranno solo essere eliminate, non modificate.

2. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI DI ASSISTENZA

ASSISTENZA TELEFONICA

Non presenta problemi da un punto di vista di trattamento di dati personali. Non sono trasmessi dati o archivi e la comunicazione rimane verbale.

ASSISTENZA TRAMITE EMAIL/TICKETS WEB

Nell'assistenza tramite e-mail i tecnici Bisy inseriranno sempre nel testo del messaggio il disclaimer per rendere edotto il Titolare dell'informativa sintetica e dei recapiti a cui potrà rivolgersi per esercitare i suoi diritti o i diritti dei suoi interessati.
L'addetto Bisy non è autorizzato a farsi mandare le credenziali di accesso del Titolare via e-mail né tantomeno potrà salvarle sullo strumento di ticketing.
Qualora un Titolare invii le credenziali di accesso al suo ambiente senza richiesta del tecnico Bisy è necessario che lo stesso risponda che non è autorizzato ad accedere ai sistemi con credenziali di altri utenti in quanto questa modalità viola il GDPR.

Gli utenti helpdesk hanno accesso completo a tutti i dati di tutte le installazioni con i loro account.
L'accesso helpdesk è con SSO tramite account aziendale e nominale di Office 365.
L'assistenza tramite ticket avviene in modo anonimo, il cliente non sa quale operatore ha risposto.
I clienti che hanno un determinato livello di servizio hanno riferimento personale con il quale dialogano costantemente per ottenere supporto nell'utilizzo della piattaforma.
Gli utenti helpdesk possono sempre "impersonare" un utente cliente tramite una funzione riservata (l'operazione è loggata ed è sempre possibile distinguere quanto fatto dall'utente vero rispetto a quanto fatto dall'helpdesk).
Non sono presenti modalità di supporto diverse da ticket/mail e telefono (quest'ultimo solo per alcuni), in quanto non ci sono installazioni presso il cliente, ma solo gestite da Bisy in Cloud.

PROGETTI DI START UP

L'attività di start up è specificata nel contratto, quindi si verifica solo il caso di:

- start up con contratto.

In tal caso le attività sono finalizzate ad adempiere all'obbligazione contrattuale e pertanto lecite.
In questo caso è necessario redigere un documento di progetto in cui si convengono con il Titolare le modalità operative di esecuzione delle attività tra cui:

- Dati personali, archivi, base dati di cui necessita l'esecuzione delle attività
- Dettaglio delle operazioni da eseguire
- Identificazione del periodo entro cui sarà terminata tale attività
- La chiusura dell'attività con la presentazione della configurazione previsione di un collaudo in cui il Titolare proverà il sistema.

I documenti che il Titolare ha sottoscritto per lo svolgimento di queste attività sono il contratto e la nomina a responsabile conferendo mandato a Bisy di svolgere tutte le attività necessarie all'erogazione del servizio.
In questo caso non serve mandare al Titolare la lettera di incarico, in quanto la stessa viene fatta da Bisy, in qualità di responsabile, agli addetti Bisy.
Con il documento "Verbale di presentazione della configurazione" e la call di presentazione della configurazione e formazione finale (che può comportare anche la modifica del verbale fino alla versione definitiva) si conclude l'attività di start up.
Nel Verbale di configurazione sono inserite le indicazioni del lavoro svolto è che è conforme rispetto all'ambito contrattuale convenuto.
Data la specificità del prodotto, la completa configurazione si vede nel tempo e con l'utilizzo della piattaforma, pertanto i dati forniti dal Titolare sono conservati per rispondere con maggiore efficienza alle richieste di verifica del cliente (ad es. per richiesta di analisi di bollette degli anni precedenti) e alla risoluzione di eventuali errori. A tal fine si informa il cliente che i dati utilizzati per il progetto di start up saranno conservati nel rispetto delle prescrizioni normative.

Tutti i documenti contenenti dati dei Titolari stampati non possono essere riutilizzati come carta da riciclo e devono essere immediatamente distrutti.

3. RESPONSABILE DEL TRATTAMENTO: MISURE DI SICUREZZA IMPLEMENTATE PER I SERVIZI SAAS - PAAS

Gli ambienti di produzione di tutti i clienti sono ospitati presso il datacenter Zucchetti, sito in Siziano (PC).

Per la soluzione fornita in modalità Saas diretta, le misure di sicurezza sono quelle del Data Center Zucchetti, come di seguito specificate:

- **Certificazioni:** Zucchetti ritiene la sicurezza un elemento prioritario e irrinunciabile per l'azienda e per i propri clienti per questo ha organizzato i propri sistemi di gestione in modo da seguire rigidi criteri di sicurezza. L'organizzazione di un sistema di gestione impone la creazione di ruoli, flussi di attività e procedure chiaramente definiti a presidio dei processi aziendali. Certificazioni: ISO 9001, ISO 27001 e ISO 22301.
- **SOC:** Il servizio SOC è operativo in logica h24 e rappresenta la struttura tecnica specializzata in tematiche Cyber Security con lo scopo dell'analisi continua delle minacce basandosi sulle informazioni tecniche generate dalle soluzioni EDR, SIEM e NTA.
- **Compliance**: i processi aziendali di Zucchetti rispondono alle normative vigenti, in particolare per quanto riguarda la rispondenza ai requisiti di privacy. In tale ambito l'azienda ha adeguato il proprio sistema di gestione alle richieste del provvedimento del Garante per la Protezione dei Dati Personali riguardo gli amministratori di sistema. Qualora le prescrizioni di legge vengano modificate Zucchetti adeguerà immediatamente le modalità di erogazione del servizio e le caratteristiche tecniche per essere conforme alle eventuali modifiche.
- **Accesso alle informazioni**: il sistema di gestione di Zucchetti prevede l'esplicita classificazione del livello di riservatezza di ogni documento. In particolare, i documenti contenenti informazioni sui sistemi di sicurezza vengono classificati come riservati e non sono diffusi all'esterno dell'azienda.
- **Accesso ai sistemi**: gli accessi ai sistemi sono sempre classificabili in accessi di produzione e accessi di amministrazione. Gli accessi di produzione sono quelli oggetto della fornitura del servizio. Gli accessi di amministrazione sono quelli effettuati da Zucchetti o dal cliente con finalità diverse quali la manutenzione, la verifica di anomalie, l'acquisizione di dati. Gli accessi di amministrazione da parte di Zucchetti sono riservati a personale con la qualifica ("ruolo") di amministratore di sistema. L'azienda pone particolare attenzione all'assegnazione di tale ruolo soltanto a personale di elevate capacità tecniche e avente caratteristiche di comprovata affidabilità e moralità. L'accesso amministrativo ai sistemi da parte di personale del cliente avverrà attraverso l'assegnazione nominale di personale a ruoli ai quali sono assegnati privilegi di accesso.
- **Auditing**: nell'ambito del proprio sistema di gestione Zucchetti pone particolare attenzione all'audit dei sistemi e delle attività amministrative compiute sugli stessi. Ogni sistema viene configurato per riportare i propri log verso un sistema centralizzato di elaborazione, classificazione e repository. Tale sistema è in grado di rilevare in tempo reale anomalie sui

sistemi. In particolare, sono riscontrabili sia eventi singoli che pattern di attività anomale quali serie di login fallite. Il sistema di gestione e analisi dei log viene inoltre utilizzato per il monitoraggio delle attività degli amministratori di sistema come prescritto dal provvedimento del Garante per la privacy. L'accesso al sistema di gestione dei log è riservato al personale di Zucchetti avente ruolo di auditor ed è inaccessibile al personale addetto all'amministrazione di sistema.

- **Riservatezza dei dati**: il presente documento è stato prodotto assumendo che i dati raccolti dal cliente e presenti sui sistemi ospitati all'interno del Datacenter siano di tipo personale/sensibile, secondo la classificazione prevista dal Codice in materia di protezione dei dati personali.
  In ogni caso Zucchetti non tratterà i dati del cliente se non per l'unica finalità della loro conservazione. Zucchetti non potrà conoscere in nessun modo i dati personali inseriti dal cliente se non previa sua autorizzazione finalizzata all'esecuzione di attività di manutenzione e assistenza dell'ambiente. Zucchetti non si assume alcuna responsabilità riguardo all'uso che di tali dati viene fatto da parte del cliente o da società incaricate dal cliente stesso che gestiscono o utilizzano il servizio ubicato e gestito nel Datacenter. Zucchetti gestirà e conserverà le informazioni in conformità alle norme espresse dalla vigente normativa.
- **Log Management**: i log dei sistemi contengono informazioni necessarie alle attività amministrative, di diagnostica e di sicurezza. I log generati da ogni sistema vengono trasferiti ad un repository centrale che ha il compito di analisi, classificazione e storage. La conservazione dei log avviene secondo le norme di legge, in particolare il Codice Privacy e le norme sulla conservazione dei dati di traffico telefonico e telematico. I log dei sistemi riportano tutte le attività significative ai fini della sicurezza quali gli accessi amministrativi, le modifiche ai permessi e alle configurazioni di sistema e di sicurezza, le anomalie. Tali log sono conservati con le stesse modalità dei log di sistema. In particolare, sono tracciate ed archiviate tutte le attività di accesso e amministrazione in conformità al provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 riguardo gli amministratori di sistema. Il sistema di repository dei log è in grado di generare alert sulla base di eventi o pattern di eventi anomali.
- **Crittografia dei dati**: di default non sono presenti sistemi di crittografia sui dati poiché per la tipologia trattata non è prevista in quanto non si tratta di dati sensibili. Tuttavia, per alcuni servizi è implementabile in relazione alle funzionalità applicative. È prevista crittografia soltanto sulle password di accesso ai vari sistemi.
- **Sicurezza dei sistemi**: i servizi di sicurezza si ritengono attivi e funzionanti a protezione delle componenti ospitate in Datacenter. I sistemi di protezione sono progettati in modo da massimizzare la protezione e sono amministrati da personale con formazione specifica che segue procedure operative stringenti.
- **Controlli di sicurezza**: Sono svolti Penetration Test a livello applicativo e Vulnerability Assessment sui sistemi con cadenza annuale in linea con le procedure ISO in essere.

- **Firewalling**: il networking del Datacenter è separato dalle reti pubbliche, dalle altre reti di Zucchetti e dalle altre reti del cliente. I flussi dati tra il networking del Datacenter e l'esterno vengono mediati da sistemi di firewall. Tali sistemi di firewall permettono il transito soltanto ai flussi dati necessari al funzionamento del servizio ed esplicitamente autorizzati.
- **Intrusion Prevention**: il Datacenter è protetto da sistemi di Intrusion Prevention System (IPS) che permettono di analizzare tutto il traffico in entrata individuando immediatamente i tentativi di attacco in corso. Il traffico di rete, su segmenti significativi della piattaforma, passa attraverso sistemi che ispezionano ogni pacchetto del traffico in transito e si comportano in modo trasparente nei confronti del traffico legittimo.
- **Filesystem Antivirus**: tutti i server dispongono di moduli Antivirus sul filesystem e, su base progettuale, possono essere configurati prodotti antivirus specifici gestiti centralmente in termini di aggiornamento, distribuzione delle policy, avvio di scansioni on demand, notifiche e gestione della area di quarantena.
- **Security Patch Management**: la piattaforma è sottoposta ad un processo periodico di verifica delle patch o delle fix rilasciate dal produttore e ritenute critiche per l'erogazione del servizio o per la sicurezza. L'applicazione delle patch verrà sottoposta a preventiva comunicazione al cliente ed effettuata mediante la pianificazione di attività di manutenzione ordinaria.
- **Sicurezza fisica**: la piattaforma hardware/software progettata fruisce di tutti i servizi di facility management del Datacenter. Di seguito sono evidenziati i 2 più importanti: rilevazione fumi e spegnimento incendi. Tutti gli ambienti della sede sono dotati di rilevatori antifumo e antincendio, con attivazione dei relativi impianti di spegnimento automatico degli incendi a saturazione di ambiente con estinguente chimico gassoso FM-200. Gli impianti garantiscono la sola disattivazione della zona oggetto dell'intervento di manutenzione. In particolare, l'impianto di spegnimento è stato progettato nel pieno rispetto della normativa UNI 9795 che garantisce la segmentazione dell'impianto e di conseguenza la perdita delle sole zone oggetto di eventuale incidente, o calamità naturale, ed il continuo funzionamento del resto dell'impianto.
- **Antiallagamento**: sono previste delle sonde di rivelazione presenza liquidi nel sottopavimento in prossimità dei raccordi, delle valvole e delle derivazioni principali dell'impianto di distribuzione dell'acqua. Eventuali fuori uscite di acqua saranno opportunamente allontanate mediante convogliamento e scarico verso l'esterno.
- **Antintrusione**: è previsto un sistema di anti intrusione integrato con l'impianto di rivelazione fumi e spegnimento incendi, con il sistema di TVCC, con il sistema di controllo accessi e con gli allarmi tecnologici. I sensori del sistema allocati all'interno dell'edificio saranno attivati e disattivati da segnali provenienti dal sistema di controllo accessi.
- **Telecamere a circuito chiuso**: le telecamere sono posizionate per il controllo del perimetro dell'edificio, degli ingressi, delle porte interbloccate e di eventuali altre zone critiche.

- **Condizionamento**: nei Datacenter di ultima generazione tutti gli impianti di condizionamento e di raffreddamento sono concepiti per poter smaltire tutta l'energia elettrica assorbita. Il limite massimo di energia termica smaltibile (media nell'area) è 2898 BTU/h per ogni metro quadro; la temperatura standard del Datacenter oscilla fra i 21 ed i 23 °C, con tolleranze di +/- 1°C.
- **Continuità ed emergenza**: il Datacenter è stato concepito per fornire affidabilità massima in termini di alimentazione dei server, in quanto ogni rack è connesso a due alimentazioni indipendenti (quadri elettrici attestati su UPS ridondati), in modo tale da permettere la manutenzione delle singole linee di alimentazione senza creare disservizio e di scongiurare blackout nel caso di fault di una linea di alimentazione. Gli interventi di manutenzione programmata comportano un fermo sulle singole alimentazioni, stimabile in circa 2 ore annue complessive. La ridondanza dell'alimentazione è ulteriormente garantita da una serie di batterie, che, nel caso di blackout di entrambe le linee di alimentazione, permettono di erogare corrente ai server per 45 minuti; in realtà tali batterie intervengono semplicemente per il tempo strettamente necessario (circa un minuto) all'entrata in regime del gruppo elettrogeno a gasolio, che ha un'autonomia di 36 ore.
- **Controllo degli accessi fisici al Datacenter**: sorveglianza armata 24 ore su 24, procedure di registrazione degli accessi e identificazione del personale che accede in nome e per conto dei clienti, accesso alle sale sistemi controllato elettronicamente tramite badge e sistemi di rilevamento di impronte digitali, controllo del perimetro con impianti a raggi infrarossi, test periodici di evacuazione, procedure di sicurezza con identificazione ed assegnazione di responsabilità.
- **Monitoraggio continuo:** tutti i sistemi sono sottoposti a monitoraggio continuo tramite software dedicato con notifiche agli amministratori in caso di rilevazione di anomalie

CONNETTIVITÀ DEL DATACENTER

- **Linee Internet**: l'ampiezza di banda è in grado di fornire il massimo delle performance in ogni circostanza. Ad oggi, al fine di assicurare funzionalità piena anche in caso di malfunzionamenti delle linee Internet di un Provider, il Data Center Zucchetti è collegato in fibra ottica con diversi fornitori di connettività e con capacità superiore ai 10 Gbit/s.
- **Disponibilità di banda**: la disponibilità di banda è garantita da monitoraggio continuativo 24x7, 365 giorni l'anno. Ogni cliente dispone di un quantitativo di banda pari al nr. di Mbit/s contrattualizzato (laddove previsto contrattualmente). Tale numero rappresenta la soglia massima di banda utilizzabile senza applicare filtri e/o blocchi sulla comunicazione, permettendo di gestire in modo dinamico eventuali picchi sul servizio erogato. Qualora il cliente superi tali "soglie" è necessario rivalutare il quantitativo di banda disponibile per la pubblicazione e/o per l'erogazione di un servizio internet.
- **IP pubblici: Zucchetti**, in qualità di Autonomous System, è in grado di offrire ip pubblici senza limitazioni e ha, qualora sia necessario, la possibilità di utilizzare gli indirizzamenti di proprietà del cliente.

- **Routing**: tutte le funzioni di routing sono garantite da apparati ridondati e configurati in modalità HSRP (Hot stand-by Routing Protocol) ove il secondario rimane in hot standby ed in grado di attivarsi automaticamente al verificarsi di un fault sul router/link primario.
- **Firewalling**: il servizio è gestito tramite sistemi ridondati al 100% prodotti da primari produttori HW internazionali. Gli stessi sono configurati in high availability in modalità Active/Passive usando il metodo LAN-Based Stateful. La sicurezza logica è garantita sia a livello perimetrale che tra i sistemi di front-end e il back-end. Sono applicate policy globali per l'inspection dei pacchetti applicando class map standard.
- **Firewall Perimetrale**: i sistemi di firewall perimetrale proteggono il Datacenter Zucchetti dalle minacce provenienti dal mondo Internet. Utilizzando le migliori tecnologie presenti sul mercato sono in grado di garantire, in ogni momento, la massima fruibilità e protezione per i servizi esposti sul web. Il servizio è ridondato in ogni suo componente, assicurando così una continua disponibilità dei sistemi.
- **Firewall di back end**: i firewall di backend forniscono un ulteriore protezione per i dati presenti all'interno del Datacenter Zucchetti. Tali dispositivi garantiscono l'integrità e la confidenzialità degli archivi presenti sui server di backend (database, file sarin …). Il servizio, ridondato in ogni suo componente, è in grado di fornire le massime performance abbinate alla massima disponibilità.
- **Sistema antintrusione**: identifica l'insieme delle strumentazioni hardware e delle configurazioni software che permettono di "tracciare" l'accesso a particolari servizi e fornire, su richiesta, l'elenco degli accessi effettuati su un particolare sistema e/o un particolare servizio.
- **AntiDDoS**: Il Datacenter Zucchetti sfrutta un servizio offerto da: FASTWEB e TELECOM, con un servizio ad alto profilo tecnologico che permette di rispondere in modo efficace alle problematiche create dagli attacchi DDoS. Inoltre, sfrutta un sistema di apparati, installati presso i DC di erogazione, ospitanti una specifica tecnologia in grado di trattare tali tipologie di minacce.
- **IDS**: nel Datacenter Zucchetti è presente un sistema IDS (Intrusion Detection System). Questo dispositivo è in grado di individuare e segnalare in tempo reale i tentativi di accesso non autorizzato. Il sistema, aggiornato in tempo reale da migliaia di sensori presenti in tutto il pianeta, è in grado di rilevare la quasi totalità delle minacce provenienti da internet (attaccchi da parte di Hacker, Virus ecc…).
- **IPS**: il sistema IPS (Intrusion Prevention System) è in grado di bloccare automaticamente gli attacchi rilevati dal dipositivo IDS, fornendo così una protezione real-time ai servizi erogati dal Datacenter Zucchetti.
- **Linee di comunicazione**: le soluzioni ed i servizi proposti possono essere erogati tramite connessione Internet protetta (https). Il cliente potrà scegliere di predisporre a propria cura e spese una linea di comunicazione VPN o MPLS.