GRUPPO SPAGGIARI PARMA
Un futuro ricco di esperienza

POLICY DI SICUREZZA

SGSI UNI CEI ISO/IEC 27001

Rev. 2.0 del 10/02/2021

Gruppo Spaggiari Parma S.p.A.
Via F. Bernini, 22/A - 43126 Parma
Tel. 0521 2992 - Fax. 0521 291657

www.spaggiari.eu

info@spaggiari.eu • spaggiari@legalmail.it
Cap. Soc. 1.200.000 € interamente versato
C.F., P.IVA e Reg. Imp. PR00150470342

REVISIONI

REV.	APPROVAZIONE DATA	APPROVAZIONE VISTO	PAG. MOD.	TIPO / NATURA DELLA MODIFICA
0.0	21/05/2018	Direzione aziendale	-	Prima stesura
1.0	18/07/2019	Direzione aziendale	All	Review del layout grafico Revisione del formato grafico del documento e della struttura societaria.
2.0	10/02/2021	Direzione aziendale	21	Introduzione delle Certificazioni ottenute dal provider Aggiunta del Cap. dedicato alle certificazioni fornite dal carrier che ospita l'infrastruttura IT.

Indice

Intro

Il presente documento descrive le **policy di sicurezza e le infrastrutture antintrusione utilizzate nei Data Center** a disposizione di Gruppo Spaggiari Parma S.p.A. Questo manuale, disponibile per la propria clientela, vuole essere un ulteriore dimostrazione di trasparenza e di affidabilità nelle infrastrutture aziendali nate per la gestione e la protezione dei dati sensibili. Tale documento non è da intendersi come sostitutivo del più corposo "*Manuale Operativo per la Sicurezza delle Informazioni*", ma parte integrante dello stesso.

Mission

Una delle "**Mission**" dei Sistemi Informativi aziendali è certamente quello di **garantire un servizio affidabile e sicuro**, ma non solo, ulteriore compito del Reparto IT è stimolare e supportare lo studio, l'analisi e la creazione di procedure alternative, per favorirne l'integrazione con gli altri processi aziendali informatici.

Obiettivi

Lo scopo del presente documento è di **presentare alcune linee guida** quale strumento utile alla stesura delle procedure sostitutive, **nell'intento di fornire un supporto ed un aiuto pratico a chi deve sviluppare procedure informatiche critiche** aziendali; le linee guida sono di natura informativa e programmatica e non precettiva, in quanto si è ben consapevoli della complessità e vastità dell'organizzazione aziendale; dei diversi assetti, degli aspetti organizzativi e funzionali delle sue strutture interne, dell'eterogeneità ed infine delle professioni in essa operanti.

Questo documento risulterà inoltre un utile strumento di sensibilizzazione in termini di sicurezza in quanto: **dà evidenza delle attività svolte dagli organi Dirigenti**; **tutela chi assume le decisioni dando prova della propria diligenza**; **fissa la conoscenza sviluppata in azienda** trasformando adempimenti dovuti per legge in valore aggiunto ed infine **permette di formalizzare le policy privacy** (corretta gestione e manutenzione).

I sistemi critici

Il presente documento analizzerà quindi **ogni policy ideata per prevenire ogni possibile criticità dell'infrastruttura IT**, proprio per questo è necessario già nella premessa definire al meglio quali sono le attività "**critiche**" secondo l'Azienda.

- L'Azienda definisce come "**Mission Critical**" i **servizi critici o le attività di supporto al Business** (interne o in outsourcing) **senza i quali l'organizzazione non può raggiungere i propri obiettivi**.

Si ricorda infine che secondo l'Agenzia per l'Italia Digitale *AgID* i sistemi "critici" non possono essere sostituiti da nulla di alternativo (solo da qualcosa di identico). Per definizione quindi i sistemi critici non prevedono nessuna procedura sostitutiva.

Aggiornamento del documento

Il presente documento sarà disponibile sia in forma cartacea presso l'Area Cloud&Infrastrutture di Gruppo Spaggiari Parma S.p.A. sia sotto forma digitale. **L'aggiornamento** dello stesso **sarà compito ed obbligo della** stessa **Area Cloud& Infrastrutture** aziendale, in modo da poter revisionare la documentazione sulla sicurezza proposta con le soluzioni più aggiornate alla data di sottoscrizione. Sarà possibile richiedere una copia digitale del presente documento scrivendo all'indirizzo e-mail: it@spaggiari.eu.

Ultimo Aggiornamento (Data – Ora – Autore): **10/02/2021** – **11:33** – **L. Todesco**

Gruppo Spaggiari Parma S.p.A.

Il **Gruppo Spaggiari Parma S.p.A. lavora nel mondo della scuola dal 1926**. Siamo da sempre focalizzati su questo mercato e l'abbiamo seguito in tutte le sue evoluzioni.

Tradizione e innovazione, da sempre

La storia della Spaggiari è sempre stata improntata ad un mix equilibrato di tradizione e innovazione. Ogni società/attività che ha aggregato nel tempo è stata **fortemente innovativa all'esordio ed ha dimostrato di sapersi rinnovare** garantendo una **perfetta sintesi di tradizione e innovazione**.

1926 - Spaggiari Registri e stampati dal 1926 progetta, produce e distribuisce registri e stampati per il mondo della scuola. Questa è stata per tantissimi anni l'attività principale e, con un catalogo di oltre 2000 prodotti e con oltre 1000 lavori personalizzati all'anno, serve con continuità più di 6000 scuole.

1949 - Spaggiari Casa Editrice pubblica manuali, libri e riviste di aggiornamento tecnico-professionale per il DSGA e il personale di segreteria. In particolare, il **Bergantini**, giunto alla 71a edizione, ha contribuito a formare intere generazioni di personale amministrativo; Pais, inoltre, rivista fondata e gestita in collaborazione con *FNADA ANQUAP*, aggiorna e informa oltre 2000 scuole.

1980 - Infoschool, **Sisdata** e **Soluzione** negli anni Ottanta hanno creato i primi software di gestione delle segreterie scolastiche e del mondo educativo; da allora sono stati protagonisti dei più importanti cambiamenti tecnologici che si sono susseguiti negli anni.

In particolare, **ClasseViva** (2009), il sistema di registro elettronico in cloud computing è stato preso a modello dal Ministero dell'Istruzione, Università e Ricerca (MIUR) per formulare la legge di Spending Review.

1991 - Edizioni Junior, editore storico della rivista Bambini, creata e diretta da Loris Malaguzzi, fondatore del Gruppo Nazionale Nidi e Infanzia a Reggio Emilia. Edizioni Junior edita e pubblica numerosi testi universitari per le facoltà di pedagogia, psicologia e scienze della formazione.

1998 - Spaggiari Distribuzione gestisce un catalogo di oltre 20.000 prodotti in pronta consegna utili per ogni necessità della scuola. Attraverso la propria piattaforma logistica cura oltre 50.000 spedizioni all'anno per oltre 500.000 righe d'ordine. Un'innovativa piattaforma cloud, progettata e gestita in proprio, integra in tempo reale scuole, reti commerciali, buyer, fornitori, produzione, logistica e spedizioni.

2001 - Italiascuola.it, società creata e gestita in collaborazione con l'Associazione nazionale Presidi (*ANP*) offre servizi di consulenza e formazione in presenza e online per Dirigenti, DSGA e alte professionalità.

Oltre 1600 scuole sono abbonate al servizio di consulenza online e oltre 3000 scuole hanno partecipato ad almeno un evento formativo organizzato da Italiascuola.it sul territorio nazionale.

2013 - Nel 2013 è stata avviata **una profonda trasformazione**, che si è completata nei primi mesi del 2014 **dando vita al Gruppo Spaggiari Parma**.

Le attività del Gruppo sono state ripensate e aggregate in cinque Divisioni che collaborano per selezionare e creare prodotti, contenuti, servizi e progetti sempre più integrati e innovativi.

Le attività operative, dall'assistenza clienti alla produzione, dagli acquisti alla logistica, dall'avvio di progetti alla consulenza direzionale sono state riorganizzate per poter offrire al cliente la massima qualità di prodotto e di servizio.

L'organizzazione commerciale di relazione con la scuola e con le comunità scolastiche è stata integrata per offrire assistenza e proattività in ognuna delle fasi della relazione commerciale. Il Gruppo potrà così soddisfare l'esigenza delle scuole di avere al proprio fianco un partner qualificato in grado di assolvere alle proprie necessità.

2017 - Nel maggio del 2017 Gruppo Spaggiari Parma S.p.A. assieme a Cooperativa Sociale Coopselios danno vita alla nuova società **Bambini S.r.l.** destinata al sistema di educazione e d'istruzione preadolescenziale, sia in ambito nazionale, che internazionale, con particolare attenzione all'innovazione tecnologica, al pensiero creativo e divergente, ai processi partecipativi e di condivisione.

Nel dicembre 2017 Gruppo Spaggiari Parma S.p.A. ha partecipato all'acquisizione di **Soluzione S.r.l. unipersonale**, società brianzola specializzata in servizi informatici, nell'ottica di rafforzare la propria posizione nel mercato delle scuole paritarie laiche e religiose. A partire dalla fine del 2017 è stata avviata una profonda riorganizzazione aziendale, che si è completata nel 2018. La nuova organizzazione ha permesso di definire tutti i prodotti e servizi offerti in tre Aree Strategiche d'Affari (**ASA**) per rispondere al meglio alle nuove esigenze del mercato.

2018 - Al termine del 2018 si concretizza un processo di scissione che esternalizza da Gruppo Spaggiari Parma S.p.A. alcune funzioni aziendali nella nuova holding industriale **Finedit Finanziaria Editoriale S.r.l.** al fine di assicurare una maggiore agilità e sviluppo organizzativo ad altre realtà aziendali accomunate dal rapporto con l'impresa emiliana.

2019 - Nell'aprile 2019 Gruppo Spaggiari Parma S.p.A. partecipa alla creazione di una nuova società dedicata al mondo assicurativo scolastico: nasce così **ABZ Broker and Consulting S.r.l.**, rivolta al mondo education e a tutti i suoi protagonisti (Dirigenti scolastici, Docenti, operatori, famiglie e studenti), destinata a migliorare i processi interni di ogni Istituto con soluzioni innovative ed attente a garantire protezione e serenità in ogni fase scolastica.

Nel dicembre 2019 **SOGI Scuola S.r.l.**, software-house veronese specializzata nel campo educativo dell'istruzione per gli adulti e nella formazione professionale in tutto il territorio nazionale, entra nell'ecosistema di Gruppo Spaggiari Parma S.p.A. ampliando i servizi offerti nel mondo scolastico al fine di offrire soluzioni personalizzate per ogni esigenza.

2020 - Nel dicembre 2020 entra a far parte dell'ecosistema di Gruppo Spaggiari Parma S.p.A. la società di consulenza **EuService S.r.l.** realtà romana incentrata sulla Gestione dei dati personali e sulla Sicurezza sul lavoro all'interno del settore scolastico nazionale.

La riorganizzazione

A partire dalla fine del 2017 è stata avviata **una profonda riorganizzazione aziendale**, che si è completata nel 2018. La nuova organizzazione permetterà di definire tutti i **prodotti e servizi** offerti **in tre Aree Strategiche d'Affari** (ASA) per rispondere al meglio alle nuove esigenze del mercato.

Il nuovo assetto societario, che ha coinvolto ogni figura e ruolo aziendale, ha permesso maggiore **agilità** e **precisione organizzativa** al fine di garantire **puntualità** e **professionalità** alla propria rete.

Oggi i ricavi sono un mix bilanciato di:

- **Infrastrutture & Tecnologie** (Hardware, Software, Sistemi, Cloud, App) 37%
- **Prodotti & Servizi** (Stampati, Badge, Libri, Riviste, Servizi, …) 37%
- **Contenuti & Consulenza** (Know-how didattico e gestionale) 26%

Nella direzione di tale riorganizzazione, Gruppo Spaggiari Parma vuole **aiutare il Dirigente Scolastico** a guidare la propria comunità verso un futuro migliore, migliorando gli ambienti della scuola, sia fisici sia virtuali. **Costruire un ecosistema digitale totalmente integrato** e supportare la crescita professionale e umana di tutto il personale della Scuola, ponendo la Scuola al centro della comunità educativa (Enti, Lavoro, …).

Policy di Sicurezza

Il problema della sicurezza di funzionamento, e cioè la **continuità operativa** e la **disponibilità di dati**, oltre che su un impianto infrastrutturale adeguato si basa anche su un'architettura informatica che permetta di **salvare i dati in modo sicuro** e ri**pristinarli quando necessario**, correlato alla **continuità di funzionamento** vi è quindi il problema di come dar fronte a disastri che minino la disponibilità dei dati aziendali e la continuità di elaborazione degli stessi.

Poiché attacchi esterni, guasti hardware o errori nelle applicazioni responsabili di crash dei sistemi e conseguente indisponibilità delle informazioni non possono essere del tutto evitati, la capacità di un'azienda a contenere tali minacce dipende dal suo stato di preparazione. Molti disastri possono essere evitati con un'attenta pianificazione, implementazione e sperimentazione di un adeguato piano di emergenza.

A prescindere dalle sue dimensioni **Gruppo Spaggiari Parma S.p.A. ha predisposto** degli **interventi significativi per assicurare una continuità operativa** capace di affrontare eventuali eventi calamitosi, grandi o piccoli che siano.

Nel documento saranno descritte le politiche di sicurezza adottate differenziando ovviamente le policy Logiche da quelle Fisiche, per queste ultime saranno infatti ulteriormente differenziati i vari **Data Center** di **Milano** (presso il comprensorio TIM S.p.A. sito a Rozzano) ed **Arezzo** (Datacenter IT1 Aruba S.p.A.).

Sicurezza Logica

La Sicurezza Logica si occupa dell'**integrità**, **disponibilità**, e **riservatezza** delle informazioni aziendali, ed è pertanto una componente estremamente critica nel processo di produzione del business. Devono essere definite adeguate policy di autenticazione ai sistemi, in grado di garantire riservatezza ed integrità dei dati trattati.

Gruppo Spaggiari Parma S.p.A. sfrutta le tecnologie più avanzate per **garantire un alto livello di servizio** in termini di tempestiva installazione di patch di sicurezza, **gestione dei sistemi di Firewalling** (in configurazione Fail-Over), **Intrusion Detection**, **sistemi di accesso remoto con VPN**, **sistemi di autenticazione** sia standard che avanzati (questi ultimi dotati di certificati digitali, doppie chiavi di accesso e Token-Card RSA Security).

La gestione della sicurezza logica dei dati viene garantita attraverso diverse policy studiate e adottate ad hoc per ogni attività, sono elencate di seguito le principali:

- Policy per l'accesso ai dati (restrizioni in base ad utenti, gruppi e postazioni);
- Regole per l'accesso alla rete dall'esterno;
- Policy dedicate per l'amministrazione remota dei Server tramite VPN;
- Policy di accesso ad Internet;
- Continuo aggiornamenti software Antivirus e relativo Database;
- Monitoraggio giornaliero dei software e delle postazioni;
- Analisi del traffico di rete (Network based);
- Intrusion Detection System (ISS Real Secure);
- Backup e Restore dei dati ove necessario.

Trattamento dei dati

Uno dei temi più importanti nella sicurezza logica, oltre che la protezione di dati dall'accesso abusivo, è sicuramente il trattamento degli stessi. L'importanza delle politiche di sicurezza aziendale adottate **in materia di trattamento dei dati** riguarda due principali settori, quello interno (inteso come sezione interna all'azienda, per semplificare idealmente identificato nella Lan aziendale) e quello esterno (inteso come l'insieme degli accessi provenienti dall'esterno della rete aziendale e quindi dall'esterno della Lan protetta).

POLICY INTERNE

Il trattamento dei dati interni nella Lan aziendale deve obbligatoriamente subire un trattamento differente da chi effettua accessi dall'esterno di tale rete. Le policy interne sono solitamente meno restrittive che verso l'esterno ed anche in questo caso si conferma tale regola. Attraverso l'**utilizzo di appositi profili informatici** e l'**adozione di un Domain Controller** è possibile assegnare **specifiche autorizzazioni agli utenti e a gruppi di utenti** (suddivisi in base al loro ruolo o al settore di appartenenza).

POLICY ESTERNE

Per quanto riguarda l'accesso ai dati dall'esterno, le policy di sicurezza risultano molto più elevate rispetto alle precedenti. Le **connessioni remote** vengono infatti **garantite attraverso connessioni VPN crittografate**. La VPN (acronimo di rete privata virtuale) è una connessione point-to-point che permette di stabilire una connessione sicura tra un pc client dell'utente ed un Server remoto aziendale utilizzando la rete pubblica di Internet.

Il Server di accesso remoto risponde alla chiamata proveniente dall'esterno richiedendo ovviamente un'**autenticazione**, solo se il client fornisce tali dati (delineati dall'Area Cloud&Infrastrutture aziendale solo ed esclusivamente a dipendenti che ne necessitano) viene stabilito un tunneling dove i dati vengono incapsulati, o racchiusi, in un'intestazione in modo da crittografarli e garantirne la riservatezza.

Si ricorda che una volta stabilita la **connessione VPN nominale 2FA con autenticazione SHA 1 e cifratura a 256 bit**, l'utente esterno sarà comunque soggetto alle **policy di trattamento dati definite all'interno della Lan aziendale** (garantendo ulteriormente la riservatezza e la sensibilità dei dati).

Sicurezza Fisica

Lo scopo principale della Sicurezza Fisica nel settore IT è quello di **proteggere i beni coinvolti nel funzionamento del processo aziendale**. In particolare, occorre definire le politiche di salvaguardia sia dei beni, che di tutti gli impianti coinvolti nel processo di produzione del business.

Le soluzioni adottate nei due Data Center sono differenti in quanto sia la loro dimensione che le loro caratteristiche risultano completamente diverse. Per questo in questo capitolo non saranno elencate tutte le policy in maniera indistinta, ma saranno proposte le soluzioni adottate nelle due location differenziandole e definendole in maniera particolareggiata.

Data Center Rozzano (MI)

Il **Data Center principale** di Gruppo Spaggiari Parma S.p.A. si trova **in housing** presso la Sede TIM S.p.A. di Via Toscana 3 a Rozzano (Milano). Tale Sala Server **rappresenta il vero core dell'azienda da cui fornisce attività di data-collection delle vendite**, sistemi a **supporto dell'Assurance** e soprattutto **servizi SaaS Cloud** per la propria clientela.

Quest'infrastruttura tecnologica d'avanguardia rappresenta un asset di grande importanza strategica per Gruppo Spaggiari Parma S.p.A. Il Data Center di TIM S.p.A. rappresenta l'**adeguata risposta** alle ns. esigenze in quanto presenta **strutture altamente industrializzate dotate dei più moderni sistemi**, **impianti** e **risorse professionali** frutto di massicci investimenti e di una esperienza pluriennale nei servizi alle imprese che assicurano elevati standard qualitativi ed una capacità complessiva di oltre 5 Gbit/s (la struttura ha ottenuto certificazioni di livello Rating 3 – former **Tier III Facility**).

In questa sezione saranno dettagliati i vari sistemi di sicurezza fisica a disposizione nel Data Center di Rozzano (Milano). Le policy di sicurezza fisica sono suddivise in base al loro settore ed al loro grado di importanza:

- Standard di Sicurezza ISO/IEC 27001-27017-27018
- Dispositivi di protezione
- Dispositivi antintrusione al Data Center
- Sistema di Alimentazione
- Rivelazione fumi e sistemi antincendio
- Sistemi di condizionamento e controllo della temperatura
- Sistemi antiallagamento.

Gestione della Sicurezza ISO/IEC 27001

Il fornitore di housing TIM S.p.A. **garantisce inoltre l'applicazione dello standard** UNI CEI EN ISO **27001**:2017 "*Information Security Management Systems — Requirements*" e quindi **la definizione ed implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni** (SGSI), assicurando il controllo dei fattori legati alla tutela delle informazioni, per quanto riguarda gli aspetti tecnologici, operativi, procedurali e umani, proponendo un approccio integrato e sistematico per poter perseguire gli obiettivi di sicurezza prefissati. Tale standard vuole quindi rappresentare non solo una certezza sulla protezione dei dati, ma un ulteriore certificazione capace di garantire ulteriormente serietà ed impegno verso la propria clientela.

Dal 6 ottobre 2003, la struttura di TIM S.p.A. si è inoltre certificata anche per le estensioni ISO/IEC **27017**:2015 "*Code of practice for information security controls based on ISO/IEC 27002 for cloud services*" e UNI CEI ISO/IEC **27018**:2019 "*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*" come linee guida della propria sicurezza delle informazioni e perseguirne la conformità.

Il provider dal 2019 è infine stato qualificato dall'Agenzia per l'Italia Digitale AgID come fornitore **IaaS** e **Cloud Services Provider** per la Pubblica Amministrazione, a riprova della bontà della propria infrastruttura e dei servizi offerti.

Dispositivi di protezione

PROTEZIONI PASSIVE:

- **Doppia recinzione esterna con grigliato metallico**, strutturata in modo da facilitarne l'ispezione visiva da parte del personale di **guardiania**, che delimita fisicamente il perimetro esterno e per altezza, spessore;
- Un **cancello esterno**, la cui apertura è a cura del **personale di sorveglianza**;
- La **portineria** è realizzata con adeguate protezioni strutturali e presenta la porta di accesso posizionata verso l'interno dell'area protetta; è, inoltre, dotata di passa-documenti per lo svolgimento delle operazioni di controllo in condizioni di massima sicurezza;
- Ingresso esterno ad accesso singolo regolamentato da un **sistema di tornelli a lettura badge**.

PROTEZIONI ATTIVE:

- **Barriere di allarme antintrusione** e/o **sistemi di video analisi avanzata**, consentono il monitoraggio di eventuali intrusioni nelle aree esterne adiacenti le sale sistemi offrendo una corretta affidabilità;
- Un **sistema di telecamere con videoregistrazione**, **barriere laser fence** e a raggi infrarossi per la **supervisione** e il **controllo del perimetro** delle sedi e/o per la verifica ed il controllo delle aree adiacenti le sale sistemi, in alcuni casi la tecnologia utilizzata è il sistema di video analisi avanzata.

PROTEZIONI ORGANIZZATIVE:

- **Presidio di sorveglianza 24 ore al giorno per tutti i giorni dell'anno**, presso la portineria centrale che supervisiona i transiti, identifica i visitatori ed eventualmente autorizza l'accesso all'interno della struttura;
- All'interno del presidio operano gli **addetti alla sorveglianza** che verificano la regolarità dei transiti con badge, nonché presiedono la gestione di tutte le operazioni richieste per l'accesso degli automezzi e dei visitatori al fine di garantire, nel rispetto delle procedure di sicurezza, l'integrazione tra i vari sistemi di protezione adottati e l'attivazione degli interventi previsti dalle procedure in vigore;
- Un **badge** definitivo **assegnato al personale** eventualmente appartenente ad una rete temporanea di impresa (RTI) previa autorizzazione attraverso sistema informatico eRAS contenente data inizio e fine validità dell'accesso ed estremi di un documento di riconoscimento della persona. Tale autorizzazione dovrà essere autorizzata da Responsabile del Centro Servizi.

Nel caso in cui il badge venga dimenticato potrà essere richiesto alla portineria un badge visitatore dietro la consegna di un documento;

- Un **badge provvisorio giornaliero** assegnato dal personale di portineria, a seguito della consegna di un documento di riconoscimento e la conferma della visita da parte del Responsabile di riferimento.
- L'RTI implementa una **politica di sicurezza degli accessi estremamente rigida** e selettiva: **possono accedere alle sedi solamente le persone precedentemente e preventivamente autorizzate** attraverso opportuni aggiornamenti dei registri elettronici (*white list*), integrati con i sistemi di tornelli a lettori di badge; l'autorizzazione e l'inserimento alla white list è soggetta ad una verifica di una *black list*.

Dispositivi antintrusione al Data Center

La Sala Server del Data Center di Rozzano (Milano) è protetta da diverse misure antintrusione. Saranno elencate di seguito le soluzioni adottate ed i relativi dettagli.

- Il **Security Operation Center** (SOC) fornito dal provider **costituisce l'elemento centrale dell'organizzazione**. Tale struttura operativa è certificata ISO/IEC 27001 per gli ambiti "*Delivery ed esercizio di soluzioni di sicurezza ICT. Esercizio di soluzioni VOIP, fonia e dati*" è composto da circa 100 specialisti che operano con un **presidio H24 7x7** in **due Control Room** dislocate rispettivamente a Milano e Roma, ha il mandato di **assicurare le attività di prevenzione e contrasto delle minacce informatiche** allo scopo di mantenere il livello di sicurezza dei servizi interni e di quelli erogati alla clientela, in linea con gli obiettivi prefissati.
- L'accesso avviene tramite porte (porte tipo REI 120) costruite in modo da resistere ad elevate sollecitazioni meccaniche e termiche;
- Le finestre e le vetrate sono dotate di apparati di sicurezza passiva (grate in ferro, vetri blindati, resistenti ad oltre 500 Joule) e/o **sistemi attivi in grado di rilevare eventuali effrazioni**;
- Sono utilizzati dei **sensori istallati su porte e finestre** (sensori magnetici, avvisatori ottici acustici e sensori RTA) collegati ad **un sistema di segnalazione degli allarmi** di tipo locale e remoto;
- Le **aree di carico e scarico** merci sono fisicamente **separate dagli altri punti di accesso** normalmente utilizzati dal personale interno ed esterno. Inoltre, per consentire un efficace monitoraggio degli accessi fisici e delle risorse è previsto l'utilizzo di un **registro degli accessi** fisici conservato in modo protetto.

È previsto un inventario di tutti i sistemi e gli apparati appartenenti all'infrastruttura IT, situati all'interno dei Data Center.

- A tutela delle misure specifiche per le apparecchiature e per l'accesso fisico è presente un **presidio armato H24 7x7 con personale di vigilanza**, con **ronde** da parte del personale di vigilanza, intensificate nelle ore notturne.

Sistemi di Alimentazione

La **continuità elettrica è garantita da 4 catene di UPS**, una da 3x800kVA e tre da 4x400kVA ciascuno, tutte **in configurazione ridondante N+1**. Tali catene sono in grado di mantenere l'intera infrastruttura a pieno regime per mezz'ora. Il sistema di batterie di backup UPS permette di gestire un blackout di oltre mezz'ora, ma normalmente entrano in funzione solo per non creare disservizio durante l'entrata in funzione dei Gruppi Elettrogeni (in ridondanza N+1) capaci di partire in meno di un minuto.

Ogni Sala Server è inoltre fornita di **sistemi ridondati di Gruppi di Continuità UPS** ed in ogni rack è presente un modulo capace di fornire ogni potenza ed assorbimento degli apparati installati. La configurazione descritta permette di erogare in media 4500 W per ogni rack, ma in caso di esigenze di potenza superiore a tale valore, la soluzione è stata progettata *ad hoc* per gestire punte fino a 5 kW su un singolo rack. Per ogni armadio sono presenti oltre 20 prese ridondate da 220V.

L'intero sistema elettrico è sottoposto ad un test mensile per garantire funzionalità e affidabilità.

Rivelazione fumi e sistemi antincendio

Tutti gli ambienti della sede sono dotati di **rilevatori antifumo** (centrale CERBERUS CT 10-03 a copertura delle sale del Data Center) **e antincendio** con attivazione dei relativi impianti di spegnimento automatico degli incendi a saturazione di ambiente con estinguente chimico gassoso FM-200. La peculiarità del FM-200 (a prevalenza di azoto) è quella di essere un gas inerte, tollerabile dall'organismo dell'uomo, e pertanto, da un lato permette che l'evacuazione delle persone sia fatta in maniera ordinata senza rischi di ressa, dall'altro non danneggia i sistemi ed è efficace nello spegnimento della fiamma.

Sistemi di condizionamento e controllo della temperatura

Gli **impianti** sono **concepiti per poter smaltire tutta l'energia elettrica degradata in calore**, al fine di garantire, sia in estate che in inverno, le seguenti condizioni ambientali:

- Temperatura 18 - 24 gradi °C;
- Umidità relativa: controllata (30-70%);
- Ricambi d'aria pari a 0.5 volumi/ora.

Sistemi 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.

Certificazioni Data Center Rozzano (MI)

Sono riportate di seguito le certificazioni emesse da un Ente qualificato terzo sulle conformità rispettate dalla Sede TIM S.p.A. ove risiede il core dell'infrastruttura IT aziendale. Per visionare il certificato aggiornato cliccare sulla rispettiva immagine.


CERTIFICATO N.
CERTIFICATE N. 9111.TEL9

TELECOM ITALIA S.p.A.
VIA GAETANO NEGRI 1 - 20123 MILANO (MI)

TIM

CLIENTELA AFFARI

VIA TONALE 11 - 20125 MILANO (MI)

ISO 9001:2015

1996-07-25 | 2019-01-29 | 2020-11-07

IAF: 31, 33, 35, 29

ISO 9001:2015


DNV·GL

MANAGEMENT SYSTEM CERTIFICATE

Si certifica che il sistema di gestione di/This is to certify that the management system of

TIM S.p.A.

Sede Legale: Via Gaetano Negri, 1 - 20123 Milano (MI) - Italy
(Riferimento al Certificato No. / Reference to Certificate No. CERT-003-2003-AIS-ROM-SINCERT)

È conforme ai requisiti della norma per il Sistema di Gestione/
Has been found to conform to the Management System standard:

UNI CEI ISO/IEC 27001:2017 (ISO/IEC 27001:2013)

Data Center & Cloud Computing Services in modalità IaaS (Infrastructure as a Service) con l'utilizzo della linea guida ISO/IEC 27018:2014., Network Services, Unified Communication & Collaboration Services, ICT Security & Mobile Services

(Settore EA: 35 - 33)

Data Center & Cloud Computing Services in Infrastructure as a Service (IaaS) service using the ISO/IEC Guide 27018: 2014 guide, Network Services, Unified Communication & Collaboration Services, ICT Security & Mobile Services

(EA Sector: 35 - 33)

Vimercate (MB), 01 dicembre 2017

Nicola Privato
Management Representative

ISO/IEC 27001:2017

Data Center Arezzo (AR)

Il **Data Center di Disaster Recovery** di Gruppo Spaggiari Parma S.p.A. si trova **in housing** presso il principale Data Center IT1 di Aruba S.p.A. (ad Arezzo). Questa installazione rappresenta la **sicurezza per la continuità di servizio dei servizi SaaS Cloud** forniti alla propria clientela.

Quest'infrastruttura tecnologica d'avanguardia rappresenta un'adeguata risposta alle **esigenze di Disaster Recovery** in quanto presenta **strutture**, **impianti** e **risorse professionali** frutto di investimenti e di una **esperienza pluriennale** nei servizi alle imprese che **assicurano elevati standard qualitativi** (la struttura ha ottenuto certificazioni di livello Rating 4 – former **Tier IV**).

In ogni modo si tratta di servizi di alta qualità **erogati da un carrier diverso da quello che fornisce il servizio principale** (e quindi diversamente soggetto a problematiche tecniche) **e** comunque **locato in una posizione geograficamente separata** (oltre 100 km dal Data Center principale).

In questa sezione saranno dettagliati i vari sistemi di sicurezza fisica a disposizione nel Data Center IT1 Aruba (Arezzo). Le policy di sicurezza fisica sono suddivise in base al loro settore ed al loro grado di importanza:

- Standard di Sicurezza ISO/IEC 27001-27017-27018 e ANSI/TIA Rating 4
- Dispositivi di protezione
- Dispositivi antintrusione al Data Center
- Sistema di Alimentazione
- Rivelazione fumi e sistemi antincendio
- Sistemi di condizionamento e controllo della temperatura

Gestione della Sicurezza ISO/IEC 27001

Il fornitore di housing Aruba S.p.A. **garantisce inoltre l'applicazione dello standard** UNI CEI EN ISO **27001**:2017 "*Information Security Management Systems — Requirements*" e quindi **la definizione ed implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni** (SGSI), assicurando il controllo dei fattori legati alla tutela delle informazioni, per quanto riguarda gli aspetti tecnologici, operativi, procedurali e umani, proponendo un approccio integrato e sistematico per poter perseguire gli obiettivi di sicurezza prefissati.

Tale standard vuole quindi rappresentare non solo una certezza sulla protezione dei dati, ma un ulteriore certificazione capace di garantire ulteriormente serietà ed impegno verso la propria clientela.

Dal 21 settembre 2018, la struttura di Aruba S.p.A. si è inoltre certificata anche per le estensioni ISO/IEC **27017**:2015 "*Code of practice for information security controls based on ISO/IEC 27002 for cloud services*" e UNI CEI ISO/IEC **27018**:2019 "*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*" come linee guida della propria sicurezza delle informazioni e perseguirne la conformità.

Il provider dal 29 marzo 2019 è infine stato qualificato dall'Agenzia per l'Italia Digitale AgID come fornitore **IaaS** e **Cloud Services Provider** per la Pubblica Amministrazione, a riprova della bontà della propria infrastruttura e dei servizi offerti.

Dispositivi di protezione

PROTEZIONI PASSIVE:

- **Recinzione esterna con grigliato metallico**, strutturata in modo da facilitarne l'ispezione visiva da parte del personale di guardiania, che delimita fisicamente il perimetro esterno;
- La **sala dati** è realizzata **ad un livello superiore a quello stradale**, in modo da prevenire possibili infiltrazioni idriche;
- La **portineria** è realizzata **con** adeguate **protezioni strutturali** e presenta la porta di accesso posizionata verso l'interno dell'area protetta; è, inoltre, dotata di passa-documenti per lo svolgimento delle operazioni di controllo in condizioni di massima sicurezza;
- **Ingresso esterno ad accesso singolo** regolamentato da un **sistema di tornelli** a **lettura badge**.

PROTEZIONI ATTIVE:

- **Barriere di allarme antintrusione** e/o **sistemi di video analisi avanzata**, consentono il monitoraggio di eventuali intrusioni nelle aree esterne adiacenti le sale sistemi offrendo una corretta affidabilità;
- Un **sistema di telecamere con videoregistrazione**, **barriere laser fence** e a raggi infrarossi per la supervisione e il controllo del perimetro delle sedi e/o per la verifica ed il controllo delle aree adiacenti le sale sistemi, in alcuni casi la tecnologia utilizzata è il sistema di video analisi avanzata.

PROTEZIONI ORGANIZZATIVE:

- **Presidio di sorveglianza 24 ore al giorno per tutti i giorni dell'anno**, presso la portineria centrale che supervisiona i transiti, identifica i visitatori ed eventualmente autorizza l'accesso all'interno della struttura;
- Un **badge** definitivo **assegnato al personale** eventualmente appartenente ad una rete temporanea di impresa (RTI) previa autorizzazione attraverso sistema informatico Aruba (https://assistenza.aruba.it/it) contenente data inizio e fine validità dell'accesso ed estremi di un documento di riconoscimento della persona;
- Un **badge provvisorio giornaliero** assegnato dal personale di portineria, a seguito della consegna di un documento di riconoscimento e la conferma della visita da parte del Responsabile di riferimento.

Sistemi di Alimentazione

La **continuità elettrica è garantita da 4,5 Mega Watt di potenza elettrica**, completamente **ridondata grazie a due Power Center Separati**. Ogni Power Center ha la capacità di alimentare separatamente il data center, anche a pieno carico, ed è dotato di sistemi UPS a doppia conversione (ridondanza tipo 2N).

Gli impianti di potenza e le batterie a servizio dei sistemi UPS si trovano in edifici dedicati e fisicamente separati tra di loro e rispetto all'edificio del Data Center, corredati anche di generatori di energia elettrica autonomi, con uno stoccaggio di carburante in grado di fornire energia per 48 ore a pieno carico senza fare rifornimento.

Rivelazione fumi e sistemi antincendio

Il Data Center è dotato di **sistemi di rilevazione ed estinzione incendi automatico** a gas inerte, innocuo per le persone e per i sistemi informatici ed **impianto di rilevazione allagamento**.

Sistemi di condizionamento e controllo della temperatura (Green Data Center)

Grande attenzione è stata posta nell'ottimizzazione del Data Center per quanto riguarda gli aspetti di risparmio energetico.

Tutto il **sistema di condizionamento** delle sale dati è realizzato **con macchine ad espansione diretta di gas ad alta efficienza**, collegate tra di loro in rete e ottimizzate da un sistema in grado di regolare la potenza di raffreddamento erogata. La struttura è dotata anche di **sistema free-cooling**. Utilizzando l'aria proveniente dall'esterno, opportunamente filtrata e corretta dal punto di vista di temperatura e umidità, è possibile ridurre al minimo l'utilizzo del sistema a pompa di calore per il raffreddamento e con esso il consumo di energia elettrica e l'impatto ambientale. Gli armadi rack che ospitano i server sono dotati di un innovativo **sistema di compartimentazione dell'aria fredda** che garantisce la massima efficienza energetica ed il comfort degli operatori.

Certificazioni Data Center Arezzo (AR)

Sono riportate di seguito le certificazioni emesse da un Ente qualificato terzo sulle conformità rispettate dalla Sede Aruba S.p.A. ove risiede il sito secondario dell'infrastruttura IT aziendale. Per visionare il certificato aggiornato cliccare sulla rispettiva immagine.


BUREAU VERITAS Certification

Allegato al Certificato di Conformità
N° IT257061/A
ARUBA SPA
Sede Legale e Operativa:
Via San Clemente, 53 - 24036 PONTE SAN PIETRO (BG)

Bureau Veritas Italia spa certifica che il sistema di gestione dell'organizzazione sopra indicata è stato valutato e giudicato conforme ai requisiti della norma di sistema di gestione seguente

Norma
ISO 9001:2015

Elenco Siti

Siti	Scopo
SITO OPERATIVO Via Gobetti, 96 52100 AREZZO (AR)	Progettazione, sviluppo ed erogazione di software e servizi di: - Data Center (Server Dedicati, Server Virtuali, Colocation, Hosting) - Soluzioni Cloud oriented in modalità IaaS, SaaS e PaaS - Posta elettronica convenzionale e certificata (PEC) - Firma digitale e firma qualificata, firma grafometrica e altre soluzioni tecnologiche di firma elettronica avanzata, firma remota, servizi di Certification Authority - Infrastrutture a chiave pubblica PKI o attinenti alla sicurezza informatica - Conservazione digitale sostitutiva - Backup e Disaster Recovery - Consulenza in ambito ICT e relativa assistenza specialistica anche tramite Call Center. Produzione e personalizzazione di carte a microprocessore (Smart Card). Commercializzazione, installazione ed assistenza di prodotti hardware e software attinenti alla sicurezza informatica. Emissione e gestione di "Identità Digitale" e delle relative credenziali di autenticazione per l'accesso ai servizi "SPID" in qualità di Identity Provider.

3/3

Rev. N. 1 del: 20 aprile 2018

ANDREA FILIPPI - Local Technical Manager

Indirizzo dell'organismo di certificazione: Bureau Veritas Italia S.p.A., Viale Monza, 347, - 20126 Milano, Italia

Ulteriori chiarimenti sul campo di applicazione di questo certificato e sui requisiti applicabili della norma del sistema di gestione possono essere ottenuti consultando l'organizzazione.
Per controllare la validità di questo certificato consultare il sito http://www.bureauveritas.it/certificate

ACCREDIA

ISO 9001:2015


BUREAU VERITAS Certification

Allegato al Certificato di Conformità
n° IT268394/A
ARUBA SPA
Sede Legale e Operativa:
Via San Clemente, 53 - 24036 PONTE SAN PIETRO (BG)

Bureau Veritas Italia Spa certifica che il sistema di gestione dell'organizzazione sopra indicata è stato valutato e giudicato conforme ai requisiti della norma di sistema di gestione seguente

Norma
ISO/IEC 27001:2013

Sito	Scopo
SEDE LEGALE E OPERATIVA Via San Clemente, 53 24036, PONTE SAN PIETRO (BG)	Progettazione, sviluppo ed erogazione di software e servizi di: - Data Center (Server Dedicati, Server Virtuali, Colocation, Hosting) - Soluzioni Cloud oriented in modalità IaaS, SaaS e PaaS - Posta elettronica convenzionale e certificata (PEC) - Firma digitale e firma qualificata, firma grafometrica e altre soluzioni tecnologiche di firma elettronica avanzata, firma remota, servizi di Certification Authority e personalizzazione di carte a microprocessore (Smart Card) - Conservazione digitale sostitutiva - Backup e Disaster Recovery e relativa assistenza specialistica. - Gestione e manutenzione di server, postazioni di lavoro, reti informatiche e relativi apparati e sistemi di sicurezza logica. - Emissione e gestione di "Identità Digitale" e delle relative credenziali di autenticazione per l'accesso ai servizi "SPID" in qualità di Identity Provider
SITO OPERATIVO Loc. Palazzetto, 4 52011 BIBBIENA (AR)	
SITO OPERATIVO Via Sergio Ramelli, 8 52100 Arezzo (AR)	
SITO OPERATIVO Via Piero Gobetti, 96 52100 AREZZO (AR)	

1/1

Rev. N. 1 del: 03 aprile 2018

ANDREA FILIPPI - Local Technical Manager

Indirizzo dell'organismo di certificazione: Bureau Veritas Italia S.p.A., Viale Monza, 347, 20126 Milano, Italia

Ulteriori chiarimenti sul campo di applicazione di questo certificato e sui requisiti applicabili della norma del sistema di gestione possono essere ottenuti consultando l'organizzazione.
Per controllare la validità di questo certificato consultare il sito www.bureauveritas.it

ACCREDIA

ISO/IEC 27001:2013

ISO 9001:2015 **ISO/IEC 27001:2013**

È possibile visionare tutte le certificazioni acquisite da Aruba S.p.A. al fine di assicurare efficacia ed efficienza delle proprie strutture Data Center selezionando il seguente link: Certificazioni Gruppo Aruba S.p.A.

Informazioni di contatto

In questo capitolo sono riportati i contatti telefonici ed e-mail di alcuni dipendenti dell'Area Cloud&Infrastrutture di Gruppo Spaggiari Parma S.p.A. Tali recapiti sono da ritenersi indispensabili **in caso di Disaster** e/o **Emergency Hardware o Software**. Tali contatti sono i principali da utilizzare per richiedere maggiori dettagli e/o delucidazioni sul presente documento e sul sistema di Sicurezza Informatica Aziendale.

CONTATTI

Il presente elenco risulterà inoltre necessario sia in caso di Disaster sia per attivare le corrette procedure di Escalation dettagliate nel "*Manuale Operativo per la Sicurezza delle Informazioni*".

Riccardo Taruffi

Resp. Area Cloud&Infrastrutture

Tel. +39 0521 299420

Mobile +39 334 6658952

taruffi@spaggiari.eu

Giovanni Culmone

Manutentore Reti & HW

Tel. +39 0521 299420

Mobile +39 335 1217281

culmone@spaggiari.eu

Informazioni sulla società

Gruppo Spaggiari Parma S.p.A.

Via Bernini 22/A, 43126 – Parma (PR)

Tel. 0521 2992

Fax 0521 291657

www.spaggiari.eu