Policy di Sicurezza

SISTEMA CLOUD SPAGGIARI - 2016

Documento Ufficiale – Gruppo Spaggiari Parma S.p.A.

Gruppo Spaggiari Parma S.p.A.

Tel. 0521949011
Fax 0521291657

Via Bernini 22A
43126 – Parma (PR)

www.spaggiari.eu
it@spaggiari.eu

Sommario

Intro 4
Premessa 4
Mission 4
Obiettivi 4
I sistemi Critici 5
Aggiornamento del documento 5
La Società 6
Gruppo Spaggiari Parma S.p.A. 6
Una lunga tradizione di eccellenza e innovazione 6
La nuova organizzazione 7
Policy di Sicurezza 8
Sicurezza Logica 9
Trattamento dei dati 9
Policy Interne 10
Policy Esterne 10
Sicurezza Fisica 11
Data Center Parma 12
Dispositivi di protezione 12
Protezioni passive: 12
Protezioni attive: 12
Protezioni organizzative: 13
Dispositivi anti intrusione Data Center 13
Sistemi di Alimentazione 14
Rivelazione fumi e sistemi anti incendio 14
Data Center Rozzano (MI) 15
Gestione della Sicurezza ISO/IEC 27001 16
Dispositivi di protezione 16

Protezioni passive: 16

Protezioni attive: 16

Protezioni organizzative: 17

Dispositivi anti intrusione Data Center 18

Sistemi di Alimentazione 19

Rivelazione fumi e sistemi anti incendio 19

Sistemi di condizionamento e controllo della temperatura 20

Sistemi anti allagamento 20

Data Center IT1 Aruba (Arezzo) 21

Gestione della Sicurezza ISO/IEC 27001 22

Dispositivi di protezione 22

Protezioni passive: 22

Protezioni attive: 22

Protezioni organizzative: 23

Sistemi di Alimentazione 23

Rivelazione fumi e sistemi anti incendio 23

Sistemi di condizionamento e controllo della temperatura (Green data Center) 24

Informazioni di contatto 25

Contatti 25

Informazioni sulla società 25

<<Il presente documento descrive le policy di sicurezza e le infrastrutture ideate per evitare ogni possibile problematica…>>

Intro

Premessa

Il presente documento descrive le policy di sicurezza e le infrastrutture anti-intrusione utilizzate nei data center a disposizione del 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 dl più corposo BCP, 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 il processo 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 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 rilegato presso l'Uff. IT del Gruppo Spaggiari Parma S.p.A. sia sotto forma digitale. L'aggiornamento dello stesso sarà compito ed obbligo del Reparto IT dell'azienda, in modo da poter aggiornare la documentazione sulla sicurezza proposta con l'attuale infrastruttura. Sarà possibile richiedere una copia digitale del presente documento in ogni momento richiedendolo tramite e-mail all'indirizzo: todesco@spaggiari.eu.

Ultimo Aggiornamento: 13/10/2016

La Società

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.

Una lunga tradizione di eccellenza e innovazione

Negli ultimi anni abbiamo aggregato in un unico Gruppo diverse società che hanno contribuito a creare la scuola così come è oggi:

- **Spaggiari Registri e stampati** che dal 1926 progetta, produce e distribuisce i registri cartacei e tutti gli stampati per il mondo della scuola.
- **Spaggiari Casa Editrice** che pubblica manuali, libri e riviste di aggiornamento tecnico professionale per il DSGA e il personale di segreteria. In particolare il Bergantini (il "must to have" delle segreterie scolastiche), giunto alla 67° edizione, ha contribuito a formare intere generazioni di personale amministrativo e il Pais, rivista gestita con FNADA ANQUAP, tiene aggiornate e informate 2000 scuole.
- **Spaggiari Distribuzione** che gestisce un catalogo di oltre 20.000 prodotti utili per ogni necessità della scuola.
- **Infoschool e Sisdata** che hanno creato i primi software di gestione segreteria negli anni ottanta e da allora sono stati protagonisti di ognuno dei cambi di tecnologia che vi sono stati negli anni. In particolare ClasseViva, il nuovo sistema di registro elettronico in cloud computing è stato preso a modello dal ministero della Pubblica Amministrazione per formulare la legge di Spending Review.
- **Italiascuola.it,** società creata e gestita in collaborazione con ANP (Associazione Nazionale Presidi) che offre servizi di consulenza e formazione in presenza e online per Dirigenti, Direttori dei Servizi Generali e Amministrativi e alte professionalità.
- **Edizioni Junior,** editore storico della rivista Bambini, fondata e diretta fino alla sua scomparsa dal fondatore degli asili di Reggio Emilia, unica grande e riconosciuta eccellenza a livello mondiale nel settore education. Edita e pubblica molti testi universitari per scienze della formazione.

La nuova organizzazione

Per aiutare le scuole ad affrontare le nuove ed impegnative sfide del futuro, abbiamo definito un organizzazione snella, coordinata e correlata ad ogni settore scolastico.

Publishing & New Media
Editoria & Nuovi Media

- **Publishing & new social media**

  Produce e distribuisce contenuti di altissima qualità. Lavora indifferentemente su ogni media (carta, e-book, siti web, app Apple e Android, social media) realizzando progetti editoriali integrati e cross mediali. In particolare aiuta le scuole ad esprimere e produrre contenuti di alta qualità.

Smart Printing Company
Registri & Stampati

- **Smart Printing Company**

  L'organizzazione della distribuzione e raccolta di informazioni è un'arte che non si improvvisa. Spaggiari progetta, produce e distribuisce su ogni media (carta, pdf, e-book, app, siti) registri e stampati utili alla scuola. In particolare sviluppa "stampati intelligenti" perfettamente integrati con le soluzioni web. Aiuta a migliorare la propria immagine e a comunicare in modo innovativo.

Infoschool
Information Technology

- **Infoschool**

  Progetta e costruisce le infrastrutture tecnologiche e i sistemi informativi per la scuola del futuro ed offre servizi a milioni di persone ogni giorno. Gestisce inoltre gestionali client e web per la corretta gestione della scuola in ottemperanza alla normativa e in coordinamento con il MIUR.

E-Distribution
Distribuzione

- **E-Distribution**

  Seleziona, rende disponibili su tutti i canali distributivi di Spaggiari (cataloghi, agenti, e-commerce, Consip, market place, ...) migliaia di prodotti utili ad ogni scuola e ad ogni persona della scuola. Dalla carta alla cancelleria, dal materiale per la didattica alle attrezzature di laboratorio, dall'hardware ai consumabili per le stampanti, dal materiale per la sicurezza al materiale di pulizia, dai libri di testo ai contenuti digitali.

Executive School mngt
Consulenza & Formazione

- **Smart School Management**

  La gestione scolastica sarà sempre più complessa e le alte professionalità della scuola necessiteranno di un aiuto nel risolvere i problemi quotidiani, cogliere le nuove opportunità e progettare una scuola migliore per tutti. Un aiuto consulenziale a ridefinire ruoli e professionalità, un sistema di aggiornamento professionale e di formazione on the job, un network di professionisti sempre a disposizione.

<<Il problema della sicurezza di funzionamento, …si basa su un'architettura informatica che permetta di salvare i dati in modo sicuro…>>

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 ripristinarli 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 il 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.

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 Parma, Milano (presso il comprensorio Telecom sito a Rozzano) ed Arezzo (Datacenter IT1 Aruba).

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.

Il 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 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 dei 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. 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 dal Reparto IT 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 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 tre Data Center aziendali 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 nei tre Data Center differenziandole e definendole in maniera particolareggiata.

Data Center Parma

Il Data Center di Parma del Gruppo Spaggiari Parma S.p.A. si trova all'interno dell'Headquarter di Via Bernini 22/A a Parma. L'area IT annessa al corpo principale dell'edificio presenta l'ingresso principale alla Sala Server non accessibile direttamente dall'esterno. Questa disposizione previene quindi accessi non autorizzati ed un controllo diretto su tale area aziendale estremamente sensibile.

In questa sezione saranno dettagliati i vari sistemi di sicurezza fisica a disposizione nella ns. Sede di Parma e nel Data Center annesso. Le policy di sicurezza fisica presenti sono suddivise in base al loro settore ed al loro grado di importanza:

- Dispositivi di protezione
- Dispositivi anti intrusione al Data Center
- Sistema di Alimentazione
- Rivelazione fumi e sistemi anti incendio
- Sistemi di condizionamento e controllo della temperatura

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 e per altezza, spessore
- Cancelli esterni, la cui apertura è a cura del personale dipendente
- Ingresso esterno con accesso regolamentato dalla portineria. L'accesso fuori dal normale orario di lavoro o turnazione viene garantito dal Custode e/o dal personale dipendente autorizzato ad accompagnare i visitatori.

Protezioni attive:

- Barriere di allarme antintrusione consentono il monitoraggio di eventuali intrusioni nelle aree esterne adiacenti al Data Center ed agli Uffici
- Barriere raggi infrarossi per la verifica ed il controllo delle aree adiacenti al Data Center

Protezioni organizzative:

- Sorveglianza del Custode che supervisiona i transiti e identifica i visitatori fuori dagli orari lavorativi e previene possibili problematiche di natura ambientale
- Tutti i visitatori sono identificati, durante l'orario lavorativo, dalla portineria e saranno accompagnati da un dipendente presso l'Ufficio che ne ha richiesto la presenza e/o l'appuntamento
- I dipendenti possono accedere in azienda esclusivamente mediante l'identificazione con l'apposito badge aziendale. L'accesso è inoltre disponibile solo tramite il tornello a tutta altezza dotato di funzionalità di interblocco a protezione dei varchi di accesso in modo da consentire l'accesso solo ad una persona alla volta
- Porta interbloccata a lettore di badge per l'accesso al Data Center. L'accesso al Data Center è consentito solo tramite Badge personale. Tutti coloro che entrano in tali aree devono esporre in maniera visibile il documento identificativo

Dispositivi anti intrusione Data Center

L'accesso ai Data Center è garantito da diversi dispositivi di protezione anti intrusione. Tali soluzioni sono da intendersi come ulteriori rispetto a quelle già elencate nella sezione dedicata alla protezione passiva.

- L'ingresso del Data Center è protetto da porta REI 120 in modo da resistere ad elevate sollecitazioni meccaniche e termiche
- L'accesso è disponibile solo al personale dipendente autorizzato dotato di proprio badge di riconoscimento e ad eventuali fornitori che dovranno sempre essere accompagnati
- Le aree di carico e scarico merci sono fisicamente separate dal Data Center. 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 ed un inventario di tutti i sistemi e gli apparati appartenenti all'infrastruttura IT, situati all'interno dei Data Center.

Sistemi di Alimentazione

Il sistema di alimentazione del Data Center di Parma è garantito dalla presenza di gruppi di continuità UPS (Uninterruptible Power Supply) ridondati capaci di mantenere l'intera infrastruttura autonoma per 10 minuti a pieno carico.

Ogni rack è dotato d prese corrente Shuko multistandard con doppio interruttore differenziale separato, eroganti FEM a 220V/16A 50Hz AC. I consumi di ogni armadio vengono verificati all'ingresso in produzione così come l'assorbimento elettrico mediante test con pistola amperometrica effettuati a campione. Tali misurazioni prevedono un tetto massimo di assorbimento a pieno regime di 2,5 KVA.

La continuità elettrica nei data center esterni è inoltre garantito a monte degli UPS da generatori Diesel ad attivazione automatica (dopo 20 secondi dall'interruzione del main power) con autonomia minima pari a 12 ore e garanzia di alimentazione carburante a quantità illimitata.

Rivelazione fumi e sistemi anti incendio

Tutti gli ambienti della Sede di Parma sono dotati di rilevatori antifumo e antincendio con attivazione dei relativi allarmi favorendo di conseguenza l’evacuazione in completa sicurezza.

Sistemi di condizionamento e controllo della temperatura

Gli impianti sono concepiti per poter mantenere temperatura costante e gradi di umidità tra il 40% ed il 60%. Tali sistemi sono ridondati in modo da prevenire eventuali problematiche. Il check delle temperature è inoltre dotato di sensori ambientali al fine di garantire, sia in estate che in inverno, le seguenti condizioni ambientali:

- Temperatura 18 - 24 gradi °C
- Umidità relativa: controllata (40-60%)

<<Il Data Center di Rozzano (Milano) rappresenta il vero core dell'Azienda…>>

Data Center Rozzano (MI)

Il Data Center principale del Gruppo Spaggiari Parma S.p.A. si trova in housing presso la Sede Telecom Italia 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 web per la propria clientela.

Quest'infrastruttura tecnologica d'avanguardia rappresenta un asset di grande importanza strategica per il Gruppo Spaggiari Parma S.p.A. Il Data Center di Telecom Italia 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.

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
- Dispositivi di protezione
- Dispositivi anti intrusione al Data Center
- Sistema di Alimentazione
- Rivelazione fumi e sistemi anti incendio
- Sistemi di condizionamento e controllo della temperatura
- Sistemi anti allagamento

<<Lo standard ISO/IEC 27001 non è solo una certezza sulla protezione dei dati, ma un ulteriore certificazione capace di garantire serietà ed impegno verso la clientela…>>

Gestione della Sicurezza ISO/IEC 27001

Il fornitore di housing Telecom Italia S.p.A. garantisce inoltre l'applicazione dello standard ISO 27001:2005 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.

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 tramite.

Protezioni attive:

- Barriere di allarme antintrusione e/o sistemi di videoanalisi 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 videoanalisi 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 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 autorizzato 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 un verifica di una black list.

Dispositivi anti intrusione Data Center

La Sala Server del Data Center di Rozzano (Milano) è protetta da diverse misure anti intrusione. 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 ed 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 permettono di gestire un black-out 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 anti incendio

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 FM200 (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 anti allagamento

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.

<<Il Data Center di Arezzo rappresenta la sicurezza per la continuità di servizio…>>

Data Center IT1 Aruba (Arezzo)

Il Data Center di DR del Gruppo Spaggiari Parma S.p.A. si trova in housing presso il principale Data Center di Aruba (Arezzo). Questa installazione rappresenta la sicurezza per la continuità di servizio dei servizi web del gruppo Spaggiari 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. 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 e ANSI/TIA rating 4
- Dispositivi di protezione
- Dispositivi anti intrusione al Data Center
- Sistema di Alimentazione
- Rivelazione fumi e sistemi anti incendio
- Sistemi di condizionamento e controllo della temperatura

<<Lo standard ISO/IEC 27001 non è solo una certezza sulla protezione dei dati, ma un ulteriore certificazione capace di garantire serietà ed impegno verso la clientela…>>

Gestione della Sicurezza ISO/IEC 27001

Il fornitore di housing Aruba S.p.A. garantisce inoltre l'applicazione dello standard ISO 27001:2005 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.

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 videoanalisi 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 videoanalisi 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 RTI previa autorizzazione attraverso sistema informatico eRAS 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 anti incendio

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 centre 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 ed 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.

Informazioni di contatto

In questo capitolo sono riportati i contatti telefonici ed e-mail di alcuni dipendenti del Reparto IT del 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 BCP.

Riccardo Taruffi
Resp. IT
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 22A
43126 – Parma (PR)
Tel. 0521949011
Fax 0521291657
www.spaggiari.eu

Firmato digitalmente da

MARIO PERETTO

O = non presente
C = IT