SIXTEMA S.P.A.

Data center

Allegato tecnico

SIXTEMA
TINEXTA GROUP

SOMMARIO

1 NOVITÀ INTRODOTTE RISPETTO ALLA PRECEDENTE EMISSIONE

Versione/Release n°	1.0	Data Versione/Release	20/07/2021
Descrizione Modifiche	Nessuna		
Motivazioni	Prima Emissione		

2 SCOPO E CONTENUTO DEL DOCUMENTO

Il documento descrive le facilities e i principi fondamentali di progettazione dei data center Sixtema.

2.1 RIFERIMENTI

Riferimento	Titolo documento	Nome file
[1]	SLA Standard	*SLA Standard_20210623.pdf*

3 INTRODUZIONE

Sixtema eroga i propri servizi attraverso due distinti data center:

⇒ **Site 1** - Data center Padova per servizi erogati in modalità SaaS (Software as a Service), IaaS (Infrastructure as a Service) e per servizi Network. La descrizione del Site 1 è riportata al § 4;

⇒ **Site 2** - Data center Modena per i servizi di Housing di sistemi server fisici di proprietà dei Clienti. La descrizione del Site 2 è riportata al § 5.

4 SITE 1 – DATA CENTER PADOVA

Il site 1 di Sixtema è ospitato all'interno del data center del Gruppo InfoCert. Tale server farm è stata progettata per erogare i servizi di business nel rispetto di elevati standard di availability e sicurezza.

L'architettura network, studiata in collaborazione con ingegneri Cisco, è realizzata su dispositivi del vendor stesso. Il layer di sicurezza perimetrale e antintrusione si basa su dispositivi Palo Alto in alta affidabilità. I DNS Infoblox permettono di rilevare, bloccare e mitigare attacchi DNS oltre ad offrire servizi integrati di sicurezza (*cloud BloxOne Threat Defense*). Il bilanciamento dei servizi e application security viene realizzato da dispositivi F5 che includono il layer Web Application Firewall (WAF).

La componente computazionale è stata realizzata su Cisco UCS al fine di supportare un'ampia scalabilità. L'infrastruttura di virtualizzazione è basata su VMware. La piattaforma storage prevede NetApp per la componente NAS e Infinidat per la parte SAN. Il backup dei dati viene effettuato su storage Data Domain. Il backup di server fisici e database viene effettuato mediante software EMC Networker e mediante Veeam il backup di server virtuali per quanto riguarda i backup, e col software Veeam. A questo è stata affiancata, per il destaging dei dati su cassetta, la tape library Quantum Scalar. Tale libreria è inoltre dotata della funzione Extended Data Life Management che consente di controllare in modo proattivo l'integrità dei dati salvati sulle cartucce a nastro.

Per il sito in oggetto è configurata la replica dei dati verso il site 2 Sixtema descritto al § 5 presso il quale vengono trasferiti i dati mediante tecnologie di replica nativa messe a disposizione dalle piattaforme di storage NAS/SAN implementate.

4.1 FACILITY MANAGEMENT

I servizi finalizzati alla gestione degli edifici e degli impianti primari (Facility Management) sono garantiti da un outsourcer che assicura l'erogazione dei medesimi. L'esternalizzazione dei suddetti servizi e delle attività primarie correlate migliorano l'efficienza dell'organizzazione interna e conferiscono una maggiore capacità adattativa in grado di rispondere efficacemente ai cambiamenti richiesti.

4.1.1 TIERING DATA CENTER

Il sito che ospita il data center, pur non essendo ufficialmente certificato, ha le caratteristiche di un data center di Tier 3.

4.1.2 ALIMENTAZIONE

I locali tecnici sono provvisti di un sistema di alimentazione elettrica progettato al fine di prevenire guasti e disservizi. L'alimentazione dei sistemi include le più moderne tecnologie al fine di incrementare l'affidabilità e assicurare la ridondanza delle funzionalità più critiche ai fini dei servizi erogati.

L'infrastruttura preposta all'alimentazione include:

- Gruppi di continuità, dotati di accumulatori, in corrente alternata (UPS);
- Disponibilità di tensione alternata (220-380V AC);
- Armadi alimentati in ridondanza con linee protette e dimensionate per l'assorbimento

concordato;

- Servizio di generatori di emergenza;
- Sistema di commutazione automatico e sincronizzazione fra generatori, rete e batterie (STS).

Ogni armadio tecnologico installato c/o il data center fruisce di due linee elettriche che assicurano l'HA in caso di interruzione di una delle due linee disponibili. L'armadio tecnologico è monitorato remotamente; vengono effettuati controlli costanti sullo stato della linea elettrica (on/off) e le potenze elettriche assorbite (ogni linea non deve superare il 50% del carico).

4.1.3 CONDIZIONAMENTO

L'area tecnica è normalmente mantenuta fra 20° e 27° con un tasso di umidità relativo compreso fra il 30% ed il 60%. Gli impianti sono dotati di batterie condensanti con sistema di raccolta e scarico condensa sigillato e controllato da sonde antiallagamento. L'intero sistema di condizionamento è asservito ai generatori di emergenza in caso di assenza di energia elettrica. Si garantisce la capacità frigorifera per armadio con un carico massimo previsto di 10KW e massimo di 15 KW su due armadi affiancati.

4.1.4 SICUREZZA ANTINCENDIO

È presente nel Datacenter un impianto di rilevazione fumi gestito da centrale analogica [NOTIFIER] con sensori ottici posizionati in ambiente e nel controsoffitto e sensori a campionamento d'aria installati sottopavimento e nelle canalizzazioni dell'aria. L'impianto di rivelazione automatica d'incendi è collegato ad impianti di spegnimento automatici a gas estinguenti ecologici con sistemi di spegnimento ad aerosol. Nel caso di intervento contemporaneo di due rivelatori nella stessa zona, è comandata la scarica di estinguente nella zona interessata. Sono presenti mezzi estinguenti portatili in conformità alle leggi e normative vigenti.

4.1.5 SICUREZZA ANTIALLAGAMENTO

Le sale sistemi sono dotate di un sistema antiallagamento realizzato mediante sonde puntuali collegate alla centralina automatica di rivelazione incendi e dislocate sottopavimento lungo la distribuzione idraulica. I condizionatori di sala sono dotati di una propria sonda antiallagamento che riporta l'allarme sul pannello di controllo della macchina stessa.

4.1.6 CERTIFICAZIONI

L'outsourcer è dotato di un sistema di Gestione della Sicurezza Informatica certificato ISO 27001.

4.2 ARCHITETTURA NETWORK

Nell'ambito della progettazione e realizzazione del data center InfoCert si è tenuto conto di tutte le best practice finalizzate alla gestione della sicurezza tra ambienti gestiti e il mondo internet. L'architettura di rete è stata progettata sfruttando i concetti di VDC e VRF:

- Virtual Device Context (VDC): Rappresenta l'unità di segregazione minima che assicura la segregazione del traffico dati tra i vari dipartimenti, la gestione separata delle configurazioni e il test di nuove configurazioni eliminando qualsiasi tipo di impatto sulla produzione;

- Virtual Routing Forwarding (VRF): È una tecnologia che abilita alla creazione di istanze multiple per il routing assicurando la loro coesistenza nello stesso router nello stesso tempo. Le istanze di routing risultano indipendenti e questo permette di evitare conflitti di indirizzamento.

Il data center si avvale di due collegamenti Gigabit Ethernet in fibra ottica su dorsali gestite da due carrier diversi. Ciascuna linea assicura una velocità di 10 Gbit/sec, eventualmente upgradabile secondo necessità. Tali collegamenti sono attestati su POP distinti, con percorsi fisici e apparati d'interfaccia separati e completamente ridondati. InfoCert è Autonomous System pertanto può gestire in maniera flessibile la fornitura di connettività Internet in termini di provider, ridondanza e bilanciamento di banda. La suddetta configurazione di rete è quella attualmente in essere; nell'ottica di un miglioramento dei servizi erogati da InfoCert, tale configurazione potrebbe essere modificata a discrezione di InfoCert sia in termini di potenziamento ed ottimizzazione delle risorse impiegate, sia in termini di disegno architetturale complessivo.

4.3 PROCESSI CHE REGOLANO LA GESTIONE DEL DATA CENTER

4.3.1 PROCEDURA DI INCIDENT MANAGEMENT

In caso di richiesta particolarmente complessa che comporti un intervento sistemistico sulle infrastrutture HW/SW dei sistemi di base e/o di rete, viene assegnato un Ticket all'area sistemistica dedicata al supporto specialistico. Le modalità di gestione dell'intervento sistemistico sono governate dal processo di Incident Management descritto nel presente paragrafo e nei seguenti. L'ambito completo del processo si applica alla gestione degli incidenti informatici che possono interessare uno o più servizi tecnologici eventualmente interconnessi. Il processo di gestione degli incidenti, condotto secondo le raccomandazioni delle Best Practice ITIL, si focalizza sulle modalità di gestione e di ripristino tempestivo degli incidenti di carattere sistemistico.

4.3.2 PROCEDURA DI PROBLEM MANAGEMENT

L'attività di Problem Management mira a ridurre gli impatti negativi a seguito di incidenti che possono essere provocati da errori/malfunzioni nelle infrastrutture IT e a prevenire il verificarsi e il ripetersi di tali errori. A tale scopo il Problem Management cerca di individuare la causa degli incidenti e ne attua le opportune azioni preventive, correttive e/o migliorative. La gestione dei problemi può essere sia reattiva che proattiva. Si ha gestione reattiva quando vengono risolti problemi a seguito di uno o più incidenti, mentre la gestione proattiva riguarda l'identificazione e la risoluzione di problemi prima che si verifichino degli incidenti.

4.3.3 PROCEDURA DI CHANGE MANAGEMENT

InfoCert mantiene un monitoraggio sull'evoluzione tecnologica per mantenere aggiornato l'hardware e il software presente nel data center con lo stato dell'arte che il mercato propone. I sistemi vengono aggiornati con le patch di sicurezza e funzionali consigliate. Tutte le eventuali modifiche alle architetture tecnologiche presenti in data center sono attuate secondo la procedura di Change Management, la quale è ispirata ai principi suggeriti dall' ITIL.

Le procedure individuate da InfoCert consentono di:

- gestire i cambiamenti all'interno del data center al fine di garantire un'efficiente gestione di tutti i cambiamenti applicativi e di infrastruttura IT e al fine di minimizzare l'impatto e gli incidenti sui servizi erogati;
- assicurare che i cambiamenti siano registrati, valutati, autorizzati, messi in priorità, pianificati, testati, implementati, documentati e revisionati in modo controllato.

4.4 GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

InfoCert è dotata di un sistema di Gestione della Sicurezza Informatica che è certificato ISO 27001. Nel seguito vengono brevemente descritte le misure di sicurezza fisica e logica adottate per difendere l'integrità e la riservatezza dei dati nonché le misure specifiche messe in opera per garantire l'aderenza alle norme prescritte dal Garante della Protezione dei dati personali.

4.4.1 SICUREZZA FISICA

Il data center di InfoCert è ospitato, in stanze separate con accesso controllato, all'interno dell'edificio situato in Padova, Corso Stati Uniti 14. Nel seguito sono descritte le modalità tecniche generali e le infrastrutture utilizzate per la sicurezza fisica del data center.

4.4.1.1 PROTEZIONE DEI LOCALI TECNICI

La zona d'ubicazione dell'immobile non presenta rischi ambientali dovuti alla vicinanza ad installazioni "pericolose". Durante la progettazione dello stabile sono stati presi opportuni accorgimenti per isolare i locali potenzialmente pericolosi, quali quelli contenenti il gruppo elettrogeno e la centrale termica. Per detti locali sono presenti le apparecchiature e gli accessori di controllo e di sicurezza previsti dalle norme in vigore. Lo stabile presenta numerose soluzioni atte ad aumentarne la sicurezza. È presente, all'interno della guardiola, un sistema di controllo in cui vengono monitorati e supervisionati i sistemi presenti (centrale antintrusione, TVCC, sistema controllo accessi). Lo stabile è costituito da due edifici che si sviluppano sopra ad un primo piano comune ad entrambi. Il primo edificio contiene prevalentemente uffici. Il secondo edificio ospita le aree in cui si svolgono le attività "sensibili". All'interno di questo secondo edificio, comprendendo il piano terra, si trova la Sala CED. Il secondo edificio è accessibile unicamente attraverso il primo.

4.4.1.2 SISTEMI ANTINTRUSIONE ESTERNA

La difesa del perimetro esterno è assicurata da:

- Una cancellata che delimita l'intero perimetro;
- Controllo perimetrale dell'edificio e degli accessi con sistema TVCC (TV a circuito chiuso);
- Lo stabile è controllato da personale 24 ore al giorno.

Le zone interne vengono monitorate tramite:

- Sensori piezodinamici per la rilevazione della rottura dei vetri;
- Rivelatori combinati microonde e infrarossi;
- Centrale antintrusione per la gestione e il controllo degli elementi in campo e la segnalazione di eventuali malfunzionamenti.

4.4.1.3 SISTEMI DI RIVELAZIONE ATTIVA E PASSIVA

I locali del data center sono tenuti sotto controllo tramite diverse tipologie di rivelatori:

- rivelatori ottici di fumo sul soffitto e nel sottopavimento;
- avvisatori manuali di allarme;
- avvisatori ottici acustici d'allarme per avviso locale;
- elaboratore per la raccolta dati, la gestione e l'autodiagnosi del sistema antincendio.

4.4.1.4 SICUREZZA DELL'EDIFICIO

Gli accessi all'edificio, durante il normale orario di lavoro, sono controllati mediante riconoscimento visivo da parte della portineria; gli accessi di personale non dipendente sono sempre subordinati ad un controllo documentale; tutti gli accessi dei dipendenti fuori orario di lavoro sono subordinati ad un controllo documentale, previa autorizzazione scritta del Responsabile della struttura di appartenenza. Il personale esterno può accedere in azienda solo se accompagnato da un Dirigente o Responsabile di Unità Organizzativa o con delega scritta firmata da un Dirigente o RSO.

4.4.1.5 SICUREZZA DELL'AREA CED

L'area CED è l'area protetta all'interno dello stabile, accessibile mediante utilizzo del badge autorizzato. Il locale è localizzato all'interno del secondo edificio citato nei precedenti paragrafi e fa parte del piano terra. All'interno di tale area si trovano la Sala CED effettiva, che contiene i dispositivi hardware e software dei diversi sistemi di InfoCert e Sixtema; una Sala di controllo in cui vengono monitorati e supervisionati i sistemi presenti (condizionamento, sistema idraulico, alimentazione elettrica e di continuità); la Sala di monitoraggio per il controllo dei sistemi di sicurezza installati. Sono autorizzate all'accesso solo le persone con ruolo operativo nell'erogazione del servizio e le persone che si occupano della gestione dell'infrastruttura. L'accesso per il personale esterno addetto alla manutenzione (interventi ordinari e straordinari) avviene unicamente in presenza di personale autorizzato ad accedere all'area CED. Vengono effettuati test periodici sull'efficacia degli allarmi installati e sulla procedura di rilascio badge adottata.

4.4.1.6 SISTEMA DI VIDEOSORVEGLIANZA SALA CED

InfoCert ha posto in essere sistemi e procedure atte a realizzare un sistema di videosorveglianza per il controllo della sala CED. La soluzione è caratterizzata dall'utilizzo di telecamere ad IP fisso e di un sistema di gestione software centralizzato. Le telecamere scelte rispondono ai requisiti studiati dal Responsabile della Sicurezza InfoCert in termini di risoluzione e sensibilità in condizioni di bassa illuminazione. Il software di gestione centralizzato consente di amministrare i parametri di registrazione e retention delle immagini acquisite. Per il controllo completo di tutte le aree interne della sala CED sono state installate telecamere IP (la cattura delle immagini avviene anche per gli spazi presenti tra le file di armadi rack).

4.4.1.7 ALIMENTAZIONE ELETTRICA - GARANZIA GRUPPI DI CONTINUITÀ

Tutte le apparecchiature del centro dati di Padova sono collegate alla rete elettrica attraverso gruppi di continuità per mantenere l'alimentazione alle apparecchiature in caso d'interruzione dell'erogazione dell'energia elettrica da parte del fornitore. Qualora l'assenza di alimentazione si

protragga per più di pochi secondi, è previsto l'avvio automatico dei gruppi elettrogeni che iniziano a fornire l'alimentazione al gruppo di continuità.

4.4.2 SICUREZZA LOGICA

Tutti i sistemi, sia quelli Linux Red Hat che quelli Windows, sono hardenizzati. A seconda della loro collocazione nell'architettura di rete (es. DMZ, Back end, etc.) è previsto un tipo di hardenizzazione diverso. L'accesso da parte degli Amministratori di sistema, all'uopo nominati, in conformità con quanto prescritto dalla normativa vigente, avviene tramite un'applicazione di *root on demand* che permette l'utilizzo dei privilegi dell'utenza root solo previa autenticazione individuale. Gli accessi sono tracciati, loggati e conservati per 6 mesi.

4.4.2.1 SICUREZZA DELLE RETI: PROTEZIONE DA INTRUSIONE

I sistemi e le reti di Sixtema sono connessi ad Internet in modo controllato da sistemi firewall che consentono di suddividere la connessione in aree a sicurezza progressivamente maggiore: rete Internet, reti DMZ (DeMilitarized Zone) o Perimetrali, Reti Interne. Tutto il traffico che fluisce tra le varie aree è sottoposto ad accettazione da parte del firewall, sulla base di un set di regole stabilite. Le regole definite sui firewall vengono progettate in base ai principi di "default deny" (quanto non è espressamente permesso è vietato di default, ovvero, le regole consentiranno solo quanto è strettamente necessario al corretto funzionamento dell'applicazione) e di "defense in depth" (vengono organizzati livelli successivi di difesa: prima a livello di rete, tramite successive barriere firewall ed, infine, a livello di sistema, tramite hardening). La definizione delle politiche di accesso relativamente ai siti del cliente saranno concordate, nel rispetto dei vincoli imposti dalle politiche di Sicurezza Informatica di InfoCert e di Sixtema, dall'area Management Information System.

4.4.2.2 SICUREZZA DEGLI ACCESSI

Il controllo dell'accesso alle informazioni avviene tramite credenziali di autenticazione rilasciate individualmente. Le credenziali sono personali e non cedibili, sono assegnate in base alla necessità di accedere ai dati o ai sistemi aziendali, sulla base del principio del "minimo privilegio". Le password sono sottoposte a policy di sicurezza stringenti (lenght, complexity, age min/max, history, tracking, ecc.). Gli utenti sono inoltre formati sui criteri di sicurezza e di custodia delle stesse. Hanno una durata massima di 6 mesi, salvo che per le persone con la nomina ad Amministratore di sistema, ai sensi dei provvedimenti del Garante per la protezione dei dati personali, la cui password dura un mese. Per i sistemi più critici è prevista l'autenticazione forte tramite token e certificati di autenticazione. I dati dei clienti memorizzati sui sistemi sono accessibili solo da parte del cliente stesso, tramite utenze personali a lui assegnate all'atto della sottoscrizione del servizio. L'autorizzazione è strettamente legata al servizio, per cui utenze relative a servizi diversi ma afferenti allo stesso cliente, a meno di diversa richiesta del cliente stesso, NON condividono gli stessi diritti di accesso.

4.4.2.3 SICUREZZA DELLE WORKSTATION

Tutte le workstation sono dotate di software antivirus con aggiornamento almeno giornaliero. Un tool automatico controlla le configurazioni, rilevando l'eventuale presenza di software non autorizzato.

4.4.2.4 AUDIT E VULNERABILITY ASSESSMENT

Un sottoinsieme delle applicazioni Sixtema erogate in modalità SaaS viene con cadenza annuale sottoposto a verifica da parte di un ente esterno tramite sessioni di Penetration Test e Vulnerability Assessment.

4.5 GESTIONE DEL PERSONALE

Il SGSI ed il Sistema di Gestione della Qualità (SGQ) hanno definito procedure stringenti per la gestione del personale, dal loro ingresso alla loro uscita. Tali procedure prevedono la gestione dell'assegnazione delle risorse individuali nonché delle credenziali e delle autorizzazioni sulla base delle effettive necessità determinate dalla collocazione prevista della persona nel contesto aziendale. Le persone sono inoltre formalmente nominate come Incaricate al trattamento ai sensi della normativa sulla protezione dei dati personali ed edotte degli obblighi che tale nomina comporta. La revisione delle autorizzazioni è svolta su base annuale. Per l'accesso ai locali e ai sistemi a supporto delle attività regolate da normativa, la revisione è almeno semestrale. Cambi di Unità organizzativa e/o dimissioni implicano l'immediata revisione/cancellazione di tutte le credenziali. Al termine del rapporto di lavoro è prevista la restituzione di tutti i beni. Eventuali eccezioni possono essere richieste alla Direzione della Sicurezza delle Informazioni, che potrà autorizzare dopo aver verificato che nessun dato aziendale possa essere esposto a rischi.

4.6 BACKUP DEI DATI

L'architettura tecnologica a servizio del processo di Backup Management utilizza tecnologie atte a garantire l'esecuzione delle copie di salvataggio. Il backup dei dati viene eseguito con modalità e pianificazione differenti a seconda della tipologia e della criticità del servizio e del dato.

4.7 BUSINESS CONTINUITY

Sixtema, al fine di prevenire che eventi disastrosi blocchino definitivamente ed irreparabilmente il proprio business, replica costantemente presso il site 2 di Modena descritto al § 5 i dati dei servizi erogati in modalità SaaS e IaaS. La replica è prevista a livello di piattaforma storage.

5 SITE 2 – DATA CENTER MODENA

Il Site 2 è ubicato in Via F. Malavolti, 5 - 41122 - Modena. Come indicato in precedenza, all'interno del site sono ospitati i sistemi server di proprietà di Clienti che hanno sottoscritto contratti di Housing.

5.1 IMPIANTO ELETTRICO

L'impianto elettrico è progettato per garantire la continuità elettrica anche in presenza di singoli fault lungo la catena di distribuzione. La configurazione in alta affidabilità è garantita da:

- due trasformatori da media a bassa tensione il primario attivo in produzione e il secondario pronto in stand by per entrare in produzione se necessario. Il trasformatore è in grado di supportare un assorbimento di corrente fino a 250 KW;
- un gruppo elettrogeno a partenza automatica per complessivi 350 KVA (280 KW con rapporto KW = KVA/1,25). Al gruppo elettrogeno viene fatta regolare manutenzione ogni 3 mesi con simulazione reale di caduta di rete elettrica in modo da constatarne l'efficienza;
- una cisterna di gasolio da 3000 litri che garantisce autonomia a fronte di assenza di corrente per circa 3 giorni. L'alimentazione del gruppo elettrogeno è garantita da contratto di fornitura del gasolio che copre 7gg/w;
- 2 gruppi UPS da 160KW ciascuno per la gestione dell'interruzione fino a un massimo di mezz'ora.
- Nella sala data center la ridondanza dell'alimentazione elettrica è realizzata tramite un sistema di distribuzione doppio radiale ridondante.

5.2 IMPIANTO DI RAFFRESCAMENTO

I locali sono condizionati con impianto ridondato di raffrescamento ad acqua, monitorato H24 che garantisce temperatura e umidità costante. Sistema di raffreddamento mirato al risparmio energetico: free cooling realizzato con 3 chiller esterni Carrier Aquasnap 39 KW e un impianto idronico che serve diverse colonnine Inrow APC all'interno del data center. Il sistema è così composto:

- Condizionamento di precisione APC InRow: sistema di raffrescamento per armadi di permutazione in una architettura in linea, che offre funzionalità quali controllo proattivo, ventole individuali sostituibili a caldo e con velocità regolabile, funzioni di gestione da remoto, protezione dal congelamento della serpentina, uscite senza tensione (contatto secco) e un percorso dei flussi d'aria orizzontale.
- Rack per dispositivi di rete e apparecchiature ad alta densità di dimensione standard: doppia linea di alimentazione proveniente da quadri elettrici separati. Le prese elettriche, ridondate, si trovano all'interno del singolo armadio.
- Gli apparati server e storage sono collocati in rack ospitati all'interno di isole a contenimento di calore (una di marca APC e una di costruzione artigianale che può ospitare rack di diverse case produttrici). Si tratta di sistemi modulari dal punto di vista del montaggio in rack e per

le unità di raffrescamento InRow. Tale infrastruttura risulta essere assemblabile in modo veloce, scalabile, modellabile a seconda del contesto.

5.3 SISTEMI DI RIVELAZIONE INCENDIO ATTIVO E PASSIVO

È presente in data center un impianto di rilevazione fumi gestito da centrale di controllo e collegato direttamente con gli impianti di spegnimento automatico degli incendi a saturazione di ambiente con estinguente chimico gassoso.

I locali del data center sono tenuti sotto controllo tramite rivelatori di fumo sul soffitto e nel sottopavimento. A fronte di eventuali allarmi sono implementati le seguenti notifiche:

- Avvisatori manuali di allarme;
- Avvisatori acustici di allarme;
- Invio automatico del messaggio di allarme all'agenzia di vigilanza;

I dati rilevati sono raccolti ed elaborati ai fini di gestione e autodiagnosi del sistema antincendio.

5.4 SISTEMI ANTIALLAGAMENTO

Il site è dotato di un sistema di rilevazione presenza acqua realizzato mediante sonde puntuali collegate alla centralina automatica di rilevazione e dislocate sotto il pavimento lungo la distribuzione idraulica.

5.5 POLICY DI ACCESSO AI LOCALI

Il data center Sixtema è ospitato in stanze separate con accesso fisico regolato da policy di security che prevedono specifiche abilitazioni per il personale esterno il quale potrà accedere solo in presenza di personale Sixtema autorizzato. Gli accessi del personale esterno dovranno essere preventivamente richiesti e formalmente autorizzati.

I soggetti incaricati della revisione legale dei conti e le Autorità di vigilanza potranno avere accesso ai dati relativi alle applicazioni ed al data center, previa richiesta al responsabile del data center, senza oneri ulteriori.

Non sono ammesse visite diverse rispetto a quelle normate senza autorizzazione del responsabile del data center.

5.6 PROTEZIONE LOCALI TECNICI

La zona d'ubicazione del site non presenta rischi dovuti alla vicinanza ad installazioni ritenute pericolose. Il gruppo elettrogeno e la centrale termica sono stati collocati a distanza di sicurezza dal data center. Tali locali ospitano le apparecchiature e gli accessori di controllo e di sicurezza previsti dalle norme vigenti. Gli impianti di raffreddamento e di antincendio con i relativi sensori di rilevazione sono separati ed autonomi rispetto a quelli dell'infrastruttura del data center.

L'edificio in cui è ubicato il data center è costruito con norme antisismiche e sorge in una zona a basso rischio idrogeologico.

5.7 SICUREZZA PERIMETRALE

Il data center è dislocato in ambiente protetto da allarmi stabilmente inseriti, strutture antisfondamento, controllo laser antintrusione, rilevatori di allarme volumetrico e accesso riservato solo a personale autorizzato come indicato al § 5.5. I locali sono presidiati internamente ed esternamente da telecamere che coprono l'intera superficie del data center. È attiva una centrale di antintrusione per la gestione ed il controllo degli elementi in campo e la segnalazione di eventuali malfunzionamenti. I sistemi di allarme sono collegati direttamente con l'istituto di vigilanza, attivo H24. Il presidio remoto, oltre alla videosorveglianza, si occupa di controllare gli accessi e riceve gli allarmi per temperature e fumi.

6 SERVICE LEVEL AGREEMENT

Il processo di Service Level Management Sixtema assicura che gli obiettivi di qualità del servizio erogato siano definiti attraverso Service Level Agreements (SLA).

Ogni KPI e SLA viene condiviso con le strutture aziendali preposte alla gestione dei livelli di servizio in modo da allineare le esigenze di business e il capacity management con i livelli di servizio garantiti da Sixtema. Per i dettagli sugli SLA dei servizi erogati si faccia riferimento all'allegato [1].