Aruba PEC S.p.A.

Addendum al Manuale di Conservazione Aruba PEC

Versione: 1.0
Data approvazione: 17/04/2019
Redazione: Enrico Gloria
Verificato da: Jessica Ferri Marini
Approvato da: Andrea Sassetti
Classificazione documento: pubblico

VERSIONE N°	DATA	NATURA DELLA MODIFICA
1.0	17/04/2019	Prima stesura

Sommario

1 Scopo

Il presente documento è l'Addendum al Manuale del sistema di conservazione del Conservatore Accreditato Aruba PEC S.p.a. (di seguito per brevità chiamato anche "Manuale").

L'Addendum descrive alcune specificità del servizio di conservazione digitale ed alcune differenziazioni nell'architettura fisica e logica per i clienti che lo adottano e contiene alcune stipule differenti da quelle del Manuale.

L'Addendum viene sottoposto all'Agenzia per l'Italia Digitale (AgID) per approvazione prima del suo inserimento all'interno delle Specifiche contrattuali (Rif. cap.10 del Manuale).

Tutte le disposizioni contenute all'interno dell'Addendum sono state oggetto di verifica e integrazione all'interno della Analisi dei Rischi e del piano della Sicurezza (rif. 12.2 del Manuale).

Il presente documento, al pari del Manuale dal quale discende, è classificato come documento pubblico.

Torna al sommario

2 Terminologia (glossario e acronimi)

2.1 Glossario dei termini e acronimi

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

2.2 Abbreviazioni e termini tecnici

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

3 Normativa e standard di riferimento

3.1 Normativa di riferimento

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

3.2 Standard di riferimento

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

4 Ruoli e responsabilità

4.1 Profili professionali all'interno della struttura organizzativa ARUBA

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

5 Struttura organizzativa per il servizio di conservazione

5.1 Organigramma

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

5.2 Strutture organizzative

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

5.3 Responsabilità e funzioni nel processo di conservazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6 Oggetti sottoposti a conservazione

6.1 Descrizione delle tipologie dei documenti sottoposti a conservazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.2 Copie informatiche di documenti analogici originali unici

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.3 Formati gestiti

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.3.1 Caratteristiche generali dei formati

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.3.2 Formati consigliati per la conservazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.3.3 Identificazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.4 Metadati da associare alle diverse tipologie di documenti

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.5 Modalità di assolvimento dell'imposta di bollo sui documenti posti in conservazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.6 Pacchetto di versamento

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.6.1 Specifiche Pacchetto di Versamento

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.7 Pacchetto di Archiviazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.7.1 Specifiche Pacchetto di Archiviazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.8 Pacchetto di Distribuzione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.9 Documenti rilevanti ai fini delle disposizioni tributarie

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.9.1 Modalità di assolvimento dell'imposta di bollo sui DIRT

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

6.10 Trattamento dei pacchetti di archiviazione contenenti documenti rilevanti ai fini delle disposizioni tributarie

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7 Il processo di conservazione

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.1.1 Ricezione dell'indice del pacchetto di versamento

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.1.2 Ricezione documenti associati ad un pacchetto di versamento

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.3.1 Specifiche rapporto di versamento

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.5 Preparazione e gestione del Pacchetto di Archiviazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.5.1 Chiusura anticipata (in corso d'anno) del Pacchetto di Archiviazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.5.2 Gestione dei Pacchetti di Archiviazione non validi o non completi

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.5.3 Rettifica dei pacchetti di archiviazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.6 Preparazione e gestione del Pacchetto di Distribuzione ai fini dell'esibizione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.6.1 Attività conseguenti alla cessazione del contratto

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.7.1 Produzione di duplicati

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.7.2 Produzione di copie

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.7.3 Produzione copie o duplicati su supporti rimuovibili

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.7.4 Intervento del Pubblico Ufficiale

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.8.1 Trasferimento dei documenti informatici in conservazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.8.2 Scarto dei documenti informatici conservati

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.8.3 Richiesta di scarto immediato

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.10 Tabella riepilogativa delle fasi del processo di conservazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

7.11 Audit Log

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

8 Il sistema di conservazione

8.1 Infrastruttura informatica datacenter

I Data Center dal quale sono erogati i servizi si trovano sul territorio nazionale e sono conformi ai requisiti della normativa ISO/IEC 27001:2013.

Nelle strutture che verranno messe a disposizione per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo sono presenti tutta una serie di sistemi che permettono di garantire integrità degli ambienti e dei servizi.

Torna al sommario

8.2 Caratteristiche generali della soluzione di conservazione

La soluzione, come meglio descritto in seguito, presenta le seguenti caratteristiche peculiari:

- architettura di produzione implementata su infrastruttura virtuale e storage dedicati predisposta totalmente ridondata (HA) presso il Data Center di proprietà del gruppo Aruba, certificato **ANSI/TIA 942-A Rating IV (ex Tier)**, sito in Ponte San Pietro (Bergamo);
- architettura secondaria predisposta per consentire la doppia scrittura del dato, effettuata attraverso procedura applicativa, e la replica sincrona storage based della piattaforma virtuale, inclusi i DB documentali e gestionali, situata presso il Data Center di proprietà del gruppo Aruba, sito in via Gobetti, Arezzo;
- una terza architettura realizzata per garantire il vaulting off-line dei dati e finalizzata ad assicurare il massimo livello di sicurezza per la disponibilità e l'accessibilità dei dati, situata presso il Data Center di proprietà del gruppo Aruba, sito in via Ramelli ad Arezzo

Il Sistema di Conservazione è sviluppato in modo modulare consentendo una facile scalabilità semplicemente aggiungendo unità e potenza elaborativa ai moduli sottoposti al maggior carico. Vista l'esperienza del Gruppo Aruba nell'ambito della gestione di grandi volumi di dati è sempre stato un obiettivo per il Gruppo creare architetture che possiamo definire elastiche: "espandibili" in caso di aumento del carico di lavoro oppure "limitabili" nel caso di una riduzione delle necessita.

L'intera soluzione è stata progettata per essere quindi in grado di gestire l'elaborazione di grandi volumi di dati, scalando sia verticalmente che orizzontalmente in ognuna delle sue singole componenti, con un elevato livello di affidabilità, distribuendo su più server fisici nodi con il medesimo ruolo ed evitando single point of failure.

L'architettura modulare del sistema è implementata al 100% su infrastruttura di virtualizzazione con hypervisor VMware e garantisce in sintesi i seguenti vantaggi:

Affidabilità - Totale ridondanza ai guasti HW

- Funzionalità di HA implementata dall'architettura virtuale.
- Almeno due moduli con il medesimo ruolo posizionati su server fisici separati.
- DBMS in configurazione Master-Master.
- Utilizzo di sistemi di firma e marca ad alte prestazioni in HA

Architettura scalabile

- Nodi di Front-End ed Application multipli e contemporaneamente attivi.
- Storage di livello Enterprise ad alte prestazioni per la piattaforma di iperconvergenza e le componenti DB
- Funzionalità di replica

Torna al sommario

8.3 Componenti Logiche

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

8.4 Componenti tecnologiche

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

8.5 Componenti fisiche

La soluzione è composta da tre infrastrutture fra loro interconnesse:

- un sito di Produzione completamente autosufficiente e con tutte le componenti ridondate in HA e collegato con linee dedicate al Datacenter Secondario di DR
- un sito Secondario di DR predisposto alla replica dei dati e con le componenti necessarie ad una ripartenza del servizio,
- il terzo sito dedicato esclusivamente al vaulting off-line dei dati

Tutte le componenti utilizzate sono di tipologia enterprise e, come tutte le soluzioni implementate da ARUBA, utilizzano prodotti di marche ampliamente riconosciute e leader del mercato di riferimento.

Torna al sommario

8.5.1 Sito Primario (Produzione)

Il sito di produzione ospita una infrastruttura virtuale basata su soluzione VMware sul quale vengono istallati:

- i nodi di Front-End per le interfacce di caricamento, esibizione e gestione,
- gli Application o Business Logic server,
- i backend server
- un cluster dedicato al DB server di ogni istanza di backend
- un nodo virtuale per la gestione delle code del sistema di caricamento,
- un nodo virtuale che implementa il DB che contiene tutte le informazioni per la gestione dell'infrastruttura (configurazione, accounting, etc.)
- Storage di livello enterprise per l'archiviazione dei documenti;
- Link ed interfacce verso i sistemi di Firma e Marcatura

Al fine di garantire i ridondanza e bilanciamento del traffico vengono utilizzati dispositivi di load balancing in grado di distribuire il carico di lavoro su un numero di macchine virtualmente illimitato. Questo meccanismo permette di risolvere oltre a problemi prestazionali con la semplice aggiunta a caldo di nuove macchine, anche problemi relativi ad eventuali guasti delle componenti bilanciate, nonché la manutenzione programmata dei singoli nodi.

Torna al sommario

8.5.2 Sito Secondario (DR)

Il sito secondario ospita un'infrastruttura virtuale basata su VMWare sulla quale vengono installati:

- Server di backend corrispondente ad uno dei nodi ridondati dell'ambiente di produzione
- Server DB sincronizzato con i DB di produzione
- Storage enterprise su cui vengono sincronizzati i dati in maniera sincrona che saranno resi disponibili ai server del sito secondario per ripristinare il servizio
- Collegamenti verso i sistemi esterni di firma e Marcatura temporale (sempre situati nel sito secondario)
- Macchine virtuali replicate dal sito primario (1 per ciascuna tipologia)

Nello specifico le macchine replicate dal sito primario sono quelle che forniscono i seguenti servizi:

- Frontend Web

- Frontend WS
- Business Logic
- Indicizzazione
- Audit
- Autenticazione

La procedura di switch tra il sito primario ed il secondario è basata tramite il cambio dei puntamenti a livello di DNS.

In caso di problemi sul sito di Produzione è possibile effettuare la riattivazione del servizio, senza perdita di dati entro 48 ore.

Torna al sommario

8.5.3 Sito di data vaulting off-line

Sul terzo sito, connesso agli altri due, è presente una Tape Library Dell (fino a LTO-8) in grado di gestire un elevatissimo numero di nastri e montarli direttamente come file system su un server specifico di appoggio (con buffer di 11 TB utili), anche mediante la tecnologia LTFS.

Torna al sommario

8.6 Procedure di gestione e di evoluzione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

8.6.1 Change management

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

8.6.2 Verifica periodica di conformità a normativa e standard di riferimento

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

9 Monitoraggio e controlli

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

9.1 Procedure di monitoraggio

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

9.2 Verifiche sugli archivi

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

9.2.1 Pianificazione delle verifiche periodiche da effettuare

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

9.2.2 Pianificazione delle verifiche periodiche da effettuare

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10 Specifiche contrattuali

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10.1.1 Nomina di Aruba quale responsabile del servizio di conservazione e del trattamento dei dati

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10.1.2 Scheda di conservazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10.1.3 Elenco Persone

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10.2 Modello di funzionamento del servizio

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10.2.1 Obblighi del Cliente

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10.2.2 Obblighi di ARUBA

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10.2.3 Compiti organizzativi

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10.2.4 Compiti di manutenzione e controllo

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10.2.5 Compiti operativi

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

10.2.6 Fasi del processo di conservazione e responsabilità

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

11 Livelli di servizio (SLA)

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12 Sicurezza del sistema di conservazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.1 Privacy e requisiti di sicurezza dei dati

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.2 Analisi dei Rischi

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.3 Controllo Accessi

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.4 Monitoraggio Eventi e Vulnerabilità di Sicurezza

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.5 Cifratura

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.6 Backup

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.7 Isolamento delle componenti critiche

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.8 Sicurezza fisica datacenter del Gruppo Aruba

Nelle tre strutture che verranno messe a disposizione per l'erogazione dei servizi viene data grande importanza alla sicurezza degli ambienti e dei dati in essi contenuti. Per questo sono presenti specifici sistemi che permettono di garantire integrità degli ambienti e dei servizi.

Quale sito primario viene utilizzato il data center Aruba situato presso Ponte San Pietro – Bergamo (DATACENTER ARUBA DC-IT3).

Il sito secondario è situato presso il data center, sempre di proprietà del Gruppo Aruba, ad Arezzo in via Gobetti (DATACENTER ARUBA DC-IT1). La struttura è in grado di attivarsi in caso di disaster recovery per garantire SLA in linea con le esigenze di operatività previste dagli Enti.

Il terzo data center, situato in via Ramelli ad Arezzo, è utilizzato quale sito dedicato al Vaulting off-line dei Dati (DATACENTER ARUBA DC-IT2).

I data center sono situati in un'area classificata come di "basso rischio idrogeologico", inoltre gli edifici sono completamente antisismici e posti ad un piano rialzato dal livello stradale, in modo da risultare maggiormente protetto alle calamità naturali.

Inoltre tutti i data center sono continuamente monitorati e dotati delle soluzioni di sicurezza più avanzate descritte in seguito.

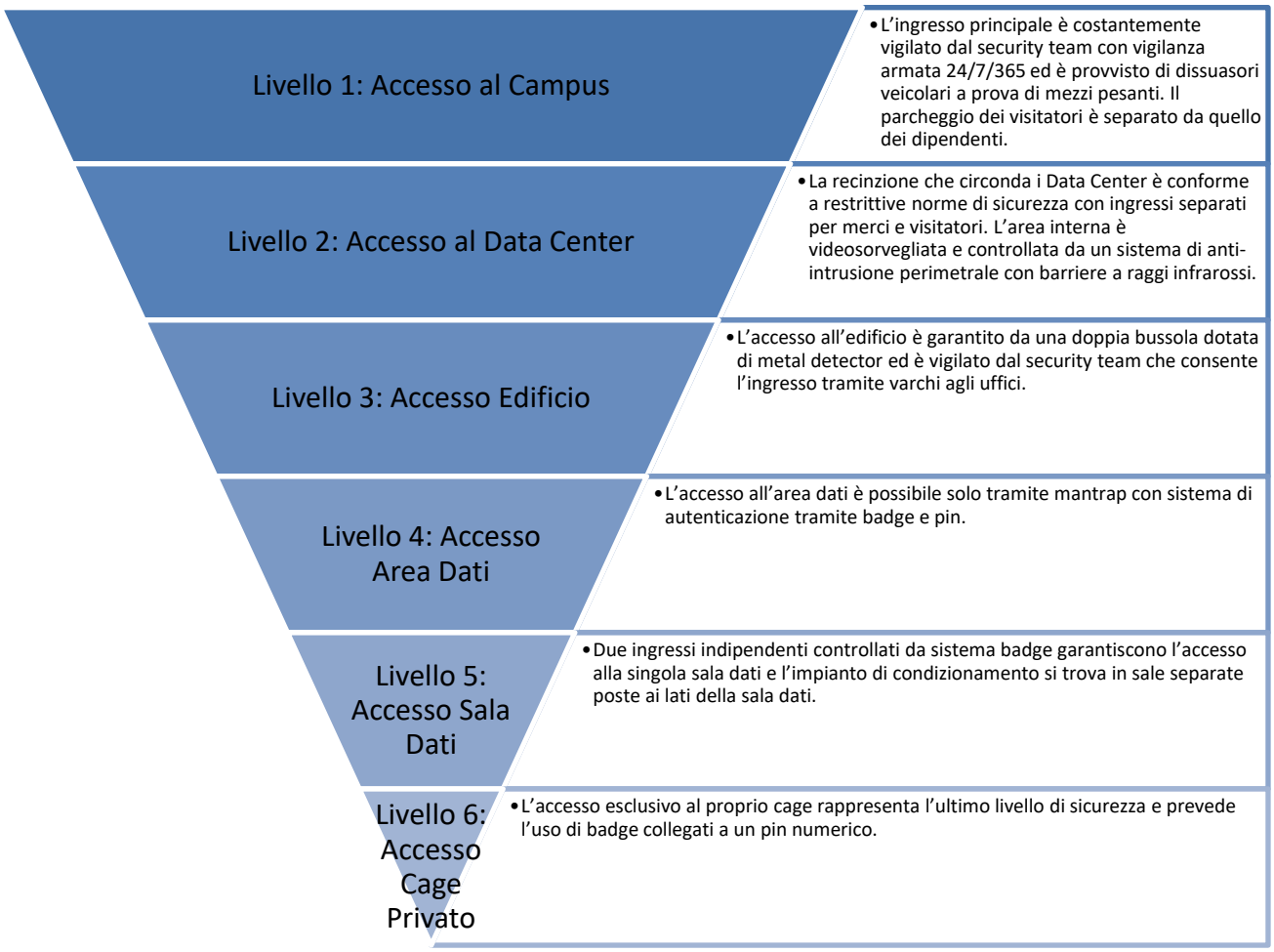
Torna al sommario

12.8.1 Sicurezza Fisica Data Center Primario

Il data center DC-IT3 è in possesso di certificazione ISO 27001 e dispone di tutte le caratteristiche principali richieste per garantire la sicurezza fisica.

Tutti gli edifici sono stati progettati per garantire il massimo della sicurezza agli ingressi: le porte esterne sono blindate, le finestre e le vetrate esterne al piano terra sono dotate di vetri antiproiettile, le griglie di areazione necessarie al raffreddamento delle sale dati sono protette da grate in acciaio.

Il perimetro del Campus è recintato e dispone di tre accessi separati. Tutte le aree esterne agli edifici presentano sistemi anti-intrusione a raggi infrarossi e di video vigilanza. Sono previsti sei livelli di sicurezza a cui corrispondono sette distinti perimetri di controllo:



I data center dispongono di un **sistema di controllo dell'accesso** esteso a tutti gli ingressi esterni (ingresso principale, uscite di emergenza, magazzini, vani e locali tecnici) e interni (sale dati, vani e locali tecnici, uffici). L'ammissione si basa su due criteri di autenticazione: una carta magnetica e una console per PIN.

Il sistema di controllo dell'accesso include l'opzione di autorizzare e disattivare le singole carte magnetiche in base ad aree, orari e altri criteri specifici, garantendo così la sicurezza completa e la praticità di accesso. È possibile generare report dettagliati (per uno specifico utente, ingresso, data) al fine di ottenere un'analisi approfondita e quanto più precisa possibile, in base alle necessità, degli spostamenti di qualsivoglia visitatore.

I cage possono essere dotati di sistemi dedicati di controllo dell'accesso, garantendo così il monitoraggio e il controllo degli accessi, nonché la capacità del visitatore di accedere autonomamente alla propria area. Sono presenti guardie armate 24 ore su 24, 7 giorni su 7.

L'edificio è dotato di un **sistema antintrusione** che impiega sensori volumetrici a doppia tecnologia, abbinati a sensori di contatto sulle finestre e sensori di vibrazione. Il sistema può contare su una tecnologia avanzata che analizza le immagini messe a disposizione dal sistema di videosorveglianza (vedere di seguito). I cortili esterni sono protetti da barriere a infrarossi lungo tutto il perimetro esterno della recinzione. Il sistema antintrusione è integrato nel sistema di controllo dell'accesso.

Il **sistema di videosorveglianza** è costituito da un determinato numero di videocamere, posizionate all'interno (lungo tutti i corridoi e nelle aree sensibili) e all'esterno (lungo il perimetro, sui tetti degli edifici e nelle aree che ospitano i generatori). Si utilizzano tipi di videocamera diversi, a seconda della diversità di caratteristiche dei vari luoghi (angolazione e distanza della visuale, tipo di illuminazione, ecc.).

Le immagini vengono messe a disposizione del personale addetto alla sicurezza in tempo reale, attraverso dei monitor del Centro Operativo. Tutte le immagini acquisite vengono archiviate su registratori digitali, conservate in aree protette e custodite per 24 ore, ai sensi degli standard applicabili per la privacy.

I server ubicati nel data center sono dotati di meccanismi di sicurezza fisica volti a prevenire il furto locale di dati. Tutti gli armadi rack sono dotati di aperture metalliche bloccabili, inoltre, i supporti di memorizzazione contenenti i dati vengono mantenuti in un luogo sicuro. Le apparecchiature di rete attive saranno ubicate all'interno di armadi di cablaggio bloccabili, impedendo così l'accesso fisico ai dischi locali e la loro rimozione.

Gli edifici DC-IT3 sono dotati di **sistemi di rilevamento del fumo** costituiti da sensori ottici posizionati negli edifici al di sotto dei pavimenti sopraelevati e al di sopra dei controsoffitti. I sensori sono collegati fra loro attraverso cavi ignifughi, in modo da rimanere operativi anche nel caso in cui un collegamento si interrompa.

Sono stati utilizzati appositi sensori per il rilevamento della presenza di fumo all'interno dei condotti di ventilazione. Il controllo del sistema viene trasferito a un'unità centrale allo scopo di rilevare eventuali segnali provenienti dai sensori, attivare gli allarmi ottici e acustici, oltre ad azionare il sistema antincendio.

Nelle aree sensibili e/o ad alto rischio (sale dati, centraline di alimentazione, cabine di trasformazione di media tensione e stanze dei quadri elettrici) è predisposto un sistema di estinzione degli incendi con gas inerte (azoto).

I **sistemi antincendio** diluiscono l'ossigeno scaricando la giusta quantità di azoto, al fine di ridurre la percentuale di ossigeno dal 23% normalmente riscontrabile nell'atmosfera a circa il 12%, impedendo in tal modo la combustione. Questo processo non presenta alcun pericolo per le persone eventualmente ancora presenti nell'area (nonostante gli allarmi ottici e acustici inviino un avviso 60 secondi prima), proteggendo inoltre le apparecchiature ed evitando pertanto l'interruzione dei servizi.

Inoltre, il sistema di estinzione degli incendi con gas inerte garantisce una doppia capacità di spegnimento. Ciò significa che all'interno del DC-IT3 sono presenti bombole sufficienti per eseguire due scariche consecutive di azoto per l'estinzione di due incendi. Questo risulta estremamente utile e si traduce come un vero e proprio sistema di ridondanza del sistema di estinzione degli incendi con gas inerte: non solo è possibile utilizzare questo sistema contemporaneamente su due aree diverse del data center, ma garantisce la costante presenza di bombole sufficienti a un secondo intervento anche nel caso la prima serie fosse stata appena utilizzata per lo spegnimento di un incendio.

I generatori di emergenza, ubicati all'esterno, dispongono di sistemi dedicati e indipendenti per il rilevamento e l'estinzione degli incendi (mediante l'utilizzo di anidride carbonica). Tali generatori sono inoltre dotati di un sistema di intercettazione del combustibile, che interrompe l'erogazione in caso di incendio. Sono presenti anche estintori portatili e mobili.

Le diverse parti degli edifici sono dotate di **sensori per il rilevamento della presenza di liquidi**, posizionati al di sotto dei pavimenti sopraelevati. Per prevenire il rischio di inondazioni causate da rotture delle tubature dell'acqua, è stato predisposto un sistema costituito da sensori (interruttori di flusso e sensori di presenza). Qualora venga rilevata la presenza di acqua, l'erogazione idraulica sarà interrotta nella stanza in questione mediante l'attivazione di una valvola solenoide, eliminando così il rischio di fuoriuscite.

In fase di progettazione, sono state indicate disposizioni anche per evitare di collocare una qualsiasi parte dei sistemi strategici al di sotto di tale posizione, eliminando pertanto l'esigenza di sistemi di prevenzione delle inondazioni che prevedano l'uso di pompe idrauliche.

Torna al sommario

12.8.2 Sicurezza fisica Data Center Secondario

Il sito secondario è situato ad Arezzo in via Gobetti ed è certificato ANSI/TIA 942-A Rating IV (ex Tier). Il datacenter è stato progettato ponendo la massima attenzione alla **sicurezza fisica degli accessi**:

- le **porte esterne** sono di tipo blindato;

- le **finestre** e le **superfici vetrate esterne** a piano terra sono dotate di vetro antiproiettile dello spessore di 21 mm;
- le **griglie per il passaggio dell'aria** necessaria al raffreddamento della sala dati sono protette da sbarre trasversali in acciaio del diametro di 20 mm.

L'**accesso dei visitatori** avviene attraverso una "**bussola**" a due ante rotanti e interbloccate, analoga a quelle normalmente utilizzate negli istituti bancari - anch'essa dotata di vetri anti-proiettile da 21 mm di spessore. Una volta avuto accesso all'interno, è presente una seconda barriera, costituita da varchi motorizzati. Per attraversare tali varchi è necessario essere accreditati alla antistante Reception, con lo scopo di ottenere un badge abilitato. Per la registrazione dei visitatori, è istituito un apposito registro conservato in conformità con quanto previsto dalla **normativa ISO 27001**.

Superata la barriera dei varchi motorizzati, si trova davanti la sala dati principale, delimitata da una parete in vetro antiproiettile da 21 mm. L'accesso, consentito solo al personale abilitato, avviene tramite porte scorrevoli di sicurezza assoggettate al controllo accessi. L'intero stabile è circondato da una resede che lo separa su tutti i lati dalle altre proprietà, e protetto da una recinzione rigida in metallo dell'altezza di 260 cm. La struttura è presidiata e sorvegliata 24x7x365.

Il **data center** è dotato di un **sistema di controllo accessi** esteso a tutti i varchi, sia esterni (ingresso principale, uscite di sicurezza, magazzini, locali tecnici) che interni (sale dati, locali tecnici, uffici). Il riconoscimento è basato su un doppio criterio di autenticazione, mediante l'utilizzo di una tessera di prossimità e la digitazione di un pin. Il sistema di gestione degli accessi prevede la possibilità di abilitare e disabilitare le singole tessere in base alle aree, agli orari ed ad altri parametri, in modo da garantire sia la massima sicurezza degli ambienti che la necessaria fluidità degli accessi. E' possibile generare dettagliati report (per utente, per varco, per data) in modo da ricostruire con la massima precisione - se necessario - i percorsi effettuati da ogni singolo visitatore.

L'edificio è dotato di un **sistema anti-intrusione** che utilizza sensori volumetrici a doppia tecnologia, assieme a sensori a contatti su infissi e sensori di vibrazione sui vetri delle sale dati.

L'impianto è integrato da sistemi evoluti di analisi delle immagini rese disponibili dall'impianto di video-sorveglianza (trattato di seguito). La resede esterna è protetta tramite barriere a raggi infrarossi applicate lungo tutto il perimetro della recinzione esterna. L'impianto anti-intrusione è integrato con il sistema di controllo accessi.

L'**impianto di video-sorveglianza** è costituito da un cospicuo numero di telecamere (oltre 120) posizionate sia all'interno dell'edificio (lungo tutti i punti di passaggio e all'interno dei locali sensibili) che all'esterno (lungo la recinzione, sulla copertura dell'edificio e nella zona dove sono ubicati i gruppi elettrogeni). Le telecamere utilizzate sono di tipologie diverse in base alle diverse esigenze derivanti dai singoli posizionamenti (angolo e distanza di visuale, tipologia di illuminazione, ecc). Le immagini vengono rese disponibili in real-time al personale di presidio mediante appositi monitor presenti all'interno del **NOC**.
Tutte le immagini acquisite vengono immagazzinate tramite videoregistratori digitali, situati in ambienti protetti e conservate per 24H, come previsto dalle vigenti **normative in ambito Privacy**.
Tutto l'edificio è dotato di un **sistema di rilevamento dei fumi** costituito da sensori ottici posizionati in ambiente, sotto al pavimento flottante e sopra il controsoffitto. I sensori sono collegati tra loro in loop e mediante cavo antifiamma, in modo da garantire il loro funzionamento anche in caso di interruzione di un collegamento. Sono stati previsti opportuni sensori in grado di verificare la presenza di fumo all'interno delle condotte per il ricambio dell'aria degli ambienti.

La gestione dell'impianto è demandata ad una centrale a 6 loop, con il compito di rilevare i segnali provenienti dai sensori, attivando gli allarmi ottici e acustici, nonché provvedendo all'attivazione dell'impianto di spegnimento mediante apposite unità di spegnimento. Le aree sensibili e/o a maggiore rischio (2 sale dati, 2 sale tlc, 6 power center, 6 sale trasformatori MT e 2 sale quadri MT) sono dotate di sistema di spegnimento a gas inerte (Azoto).

Il **metodo di spegnimento** è quello della diluizione d'ossigeno, ottenuto mediante una scarica di un'adeguata quantità di azoto in grado di ridurre la percentuale di ossigeno dal 23% presente normalmente in atmosfera al 12% circa, valore che non consente la combustione. Tale scarica non rappresenta un pericolo per la salute delle persone eventualmente ancora

presenti nell'ambiente al momento della scarica (comunque annunciata con un anticipo di 60 secondi da allarmi acustici e ottici) e preserva gli apparati consentendo la continuità nell'erogazione dei servizi.

I gruppi elettrogeni di emergenza presenti, posizionati all'esterno, sono dotati di impianti di rilevazione e di spegnimento incendi (ad anidride carbonica) dedicati e autonomi. Tali gruppi sono dotati inoltre di sistema di intercettazione del carburante, in grado di interrompere l'afflusso in caso di incendio. E' inoltre presente la normale dotazione di estintori portatili e carrellati.

I vari locali dell'edificio sono dotati di sensori per il **rilevamento della presenza di liquidi**, posizionati sotto il pavimento flottante. Per quanto riguarda la possibilità di allagamento derivante da rottura delle tubazioni per l'acqua dei servizi igienici (o dalla dimenticanza di rubinetti aperti), è stato previsto un sistema costituito da sensori (flussostati e rilevatori di presenza) e da una logica che, nel caso in cui venga rilevato il flusso di acqua in assenza di persone all'interno dei singoli servizi igienici, provvede all'interruzione dell'erogazione dell'acqua nel medesimo ambiente tramite l'attivazione di una elettrovalvola, eliminando la possibilità di riversamento di acqua a terra.
Le eventuali problematiche derivanti da alluvioni sono scongiurate, in quanto la struttura è ubicata in zona pianeggiante ed in posizione rilevata di circa un metro rispetto al piano di campagna. In fase progettuale si è provveduto inoltre a evitare il posizionamento di impianti strategici o di parte di essi a quota inferiore a tale valore: ciò esclude la necessità di sistemi anti-allagamento dotati di pompe idrauliche.

I server dislocati presso il Centro Servizi saranno dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati. Gli armadi rack sono tutti dotati di sportelli metallici con serratura a chiave e i supporti di memorizzazione contenenti dati sono conservati in luogo sicuro. Gli apparati attivi di rete saranno posizionati in armadi di cablaggio con chiusura a chiave che inibisce l'accesso fisico ai dischi locali e ne impedisce la rimozione.
Tutti gli impianti sopradescritti, assieme agli impianti e sistemi strategici (gruppi elettrogeni, ups, quadri elettrici, condizionamento di potenza) e agli impianti standard (illuminazione, condizionamento uffici) sono supervisionati da un sistema **BMS** (**Building Management System**) a mappe, in grado di gestire tutti gli eventi e gli allarmi, di interpretarli e di assegnare loro le opportune priorità, generando le conseguenti notifiche in modo da ridurre al massimo i tempi di interpretazione e individuazione degli eventi. Il **BMS** - controllato dal personale di presidio del **NOC** (**Network Operation Center**) - è accessibile anche da remoto ed in grado di provvedere alla notifica degli allarmi tramite i consueti canali (e-mail, SMS, ecc).

La pavimentazione flottante è realizzata mediante pannelli in conglomerato ad alta resistenza appoggiate su struttura composta da tubolari in acciaio ed offre adeguate capacità di carico e di resistenza. Al fine di verificare la corrispondenza con i dati del fornitore sono state eseguite prove di carico in laboratorio.

Torna al sommario

12.8.3 Sicurezza fisica del terzo Data Center

La **sicurezza fisica** del terzo **data center** viene garantita attraverso:

- un sistema di video-sorveglianza che utilizza telecamere motorizzate per tenere sotto controllo i punti nevralgici della struttura;
- un sistema di allarme che rileva automaticamente eventuali vibrazioni o aperture non autorizzate di ingressi e di infissi;
- un impianto anti-intrusione – monitorato dal NOC - che utilizza rilevatori di presenza a doppia tecnologia (micro-onde e raggi infrarossi), contatti magnetici e barriere a raggi infrarossi per proteggere le zone in cui gli ambienti sono suddivisi e prevenire l'apertura non autorizzata di ingressi ed infissi;
- sistema di controllo accessi che permette l'accesso al solo personale autorizzato, dotato di badge con tecnologia RFID e codice PIN personale;
- un sistema anti-incendio a gas inerti (non tossici) - connesso a rilevatori di fumo posti sopra e sotto al pavimento flottante – che si attiva automaticamente inondando di gas solo la zona colpita;

- un sistema di rilevazione liquidi che permette di intercettare - dal NOC e tramite appositi allarmi acustici in loco - eventuali fuoriuscite di liquido dagli impianti tecnologici;
- un sistema centrale server per archiviare e consultare (da personale autorizzato tramite accesso protetto) qualsiasi accesso ai locali, che solo avviene attraverso RFID associato a codice numerico.

Anche in questo sito, i server sono dotati di meccanismi di sicurezza fisica utili ad impedire il furto locale dei dati: gli armadi rack sono provvisti di sportelli metallici con serratura a chiave; i supporti di memoria dati sono conservati in un luogo sicuro ed i server sono protetti da un apposito sportello con chiusura a chiave (come inibizione dell'accesso fisico e della rimozione).

Torna al sommario

12.8.4 Sicurezza organizzativa comune ai data center

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.8.5 Sicurezza Logica dei sistemi e degli apparati

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.9 Piano di Disaster Recovery e Continuità operativa

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.9.1 Business Impact Analisys (BIA)

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.9.2 Analisi dei Rischi

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.9.3 Classificazione dei Sistemi e delle Risorse

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

12.9.4 Modalità tecniche per la Business Continuity ed il Disaster Recovery

Come descritto nell'architettura fisica della soluzione il sistema di produzione è completamente ridondato senza alcun Single Point of Failure, inoltre l'impatto sulle performance dovuto alla rottura di un singolo componente può essere considerato irrilevante e comunque la configurazione normale ripristinata nel giro di pochi minuti.

STORAGE DI CONSERVAZIONE: La seconda copia storage del sistema di conservazione risiede sul sito di DR ed è una copia sincrona dello storage primario. In caso di Disastro lo storage del sito secondario, che conserva tutti i dati online, è dunque già pronto ad essere utilizzato e viene semplicemente connesso via NFS all'ambiente di gestione. Essendo in copia sincrona non è prevista perdita di dati.

METADATI E ALTRI DATABASE: Il database NoSQL presente sul sito di Produzione è distribuito su più nodi fisici e più copie e dunque privo di single point of failure, inoltre replica in maniera applicativa asincrona il DB di produzione su altre VM NoSQL sempre attive sul sito di DR.

Gli altri database transazionali sono realizzati in Produzione su ambiente virtuale privo di point of failure ed in grado di riattivarsi in caso di failure in pochi secondi, inoltre viene replicato in DR mediante meccanismi di log shipping.

ALTRE VM COMPONENTI IL SERVIZIO DI CONSERVAZIONE E PORTALE DI GOVERNANCE: Tutti gli altri sistemi risiedono nel cluster di virtualizzazione in completa ridondanza e alta affidabilità, che viene inoltre replicato verso il sito di DR

Torna al sommario

13 Normative in vigore nei luoghi dove sono conservati i documenti

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

14 Disposizioni finali

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

14.1 Nullità o inapplicabilità di clausole

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

14.2 Interpretazione

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

14.3 Nessuna rinuncia

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

14.4 Comunicazioni

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

14.5 Intestazioni e Appendici e Allegati del presente Manuale Operativo

Non applicabile

Torna al sommario

14.6 Modifiche del Manuale di conservazione e del presente addendum

ARUBA si riserva il diritto di aggiornare periodicamente il *Manuale di conservazione* ed il presente Addendum, in modo estensibile al futuro e non retroattivo. Le modifiche sostituiranno qualsiasi disposizione in conflitto con la versione di riferimento del *Manuale* di conservazione e dell'Addendum.

Torna al sommario

14.7 Violazioni e altri danni materiali

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario

14.8 Norme Applicabili

Nessuna variazione rispetto a quanto descritto nel Manuale di Conservazione

Torna al sommario