



# REVAMP INFRASTRUTTURA IT

Spett.le  
**Comune di Monte Isola**  
Località Siviano, 76, 25050 Monte Isola BS  
CF00830780177



**Autore** [filippo.mascoli@tier1.it](mailto:filippo.mascoli@tier1.it)  
[alessandro.rumi@tier1.it](mailto:alessandro.rumi@tier1.it)

**Revisione** 2025-12-18

**Livello di confidenzialità** Riservato

## 1. EXECUTIVE SUMMARY

Il presente capitolo fornisce una visione d'insieme del progetto di revamp dell'infrastruttura IT del Comune di Monte Isola, sintetizzando gli interventi previsti, i benefici attesi e le motivazioni strategiche alla base delle scelte tecnologiche. L'Executive Summary è pensato per fornire ai decisori una comprensione immediata del valore del progetto, rimandando alle sezioni successive per i dettagli tecnici e implementativi.

### 1.1 sintesi del progetto

Il presente documento descrive il progetto di modernizzazione dell'infrastruttura IT del Comune di Monte Isola, un ente locale situato nella provincia di Brescia. L'intervento mira a garantire sicurezza, affidabilità e conformità normativa attraverso l'adozione di tecnologie moderne e l'implementazione di best practice di settore.

Il progetto nasce dalla necessità di rispondere a un contesto tecnologico ormai obsoleto e a un panorama di minacce cyber in costante evoluzione. Gli enti pubblici italiani sono sempre più nel mirino di attacchi informatici, in particolare ransomware, che possono paralizzare i servizi ai cittadini e comportare gravi conseguenze in termini di perdita di dati, sanzioni normative e danno reputazionale. Il Comune di Monte Isola, pur essendo un ente di piccole dimensioni, tratta dati sensibili dei cittadini e deve garantire la continuità dei servizi essenziali: anagrafe, servizi finanziari, biblioteca, informazioni turistiche.

La strategia proposta si basa su tre pilastri fondamentali: - **Protezione**: implementazione di difese moderne a livello di rete, endpoint e identità - **Migrazione cloud**: spostamento dei servizi core verso piattaforme affidabili e certificate - **Resilienza**: backup e procedure di disaster recovery per garantire la continuità operativa

### 1.2 principali interventi

Area	Intervento
Network Security	Implementazione firewall Fortinet con SD-WAN, switch gestiti e WiFi segmentato
Endpoint Security	Protezione EDR/XDR con SentinelOne Complete
Cloud	Migrazione posta elettronica e dati su Microsoft 365
Identity	Migrazione Domain Controller in datacenter certificato ISO 27001
Backup	Soluzione di backup cloud per Microsoft 365

### 1.3 Benefici attesi

- **Sicurezza rafforzata**: Protezione multilivello contro minacce cyber
- **Alta disponibilità**: Firewall in HA nella sede principale, servizi cloud ridondati
- **Conformità**: Allineamento alle linee guida AGID e normativa GDPR

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

[hello@tier1.it](mailto:hello@tier1.it)  
[www.tier1.it](http://www.tier1.it)





- **Efficienza operativa:** Gestione centralizzata e monitoraggio proattivo
- **Continuità operativa:** Backup e disaster recovery per dati critici

## 2. CONTESTO E OBIETTIVI

Comprendere il contesto di partenza è fondamentale per apprezzare la portata degli interventi proposti e le motivazioni che li rendono necessari. Il Comune di Monte Isola, situato sull'omonima isola lacustre nel Lago d'Iseo, rappresenta una realtà unica nel panorama italiano e attira ogni anno migliaia di turisti. Questa peculiarità geografica, se da un lato costituisce un'attrattiva, dall'altro pone sfide specifiche in termini di connettività e continuità dei servizi.

L'infrastruttura IT attuale riflette scelte tecnologiche effettuate anni fa, quando le esigenze di sicurezza informatica e le minacce cyber erano radicalmente diverse. Oggi, con l'aumento esponenziale degli attacchi alla Pubblica Amministrazione italiana e con l'evoluzione normativa (GDPR, direttive AGID, Piano Triennale), è indispensabile un intervento strutturale che porti l'infrastruttura del Comune a uno standard adeguato ai tempi.

### 2.1 Situazione attuale

Il Comune di Monte Isola dispone attualmente di: **3 sedi operative:** Municipio (principale), Biblioteca, Infopoint, **~15 utenti** distribuiti prevalentemente nella sede principale, **Domain Controller** su Windows Server 2008 R2 (end of support), **Posta elettronica** su Aruba, **Applicativi legacy** (Sicraweb, Re-Rite, Concilia) su server locale, **Infrastruttura di rete** datata e non segmentata.

### 2.2 Incidente di Sicurezza - Gennaio 2025

**NOTA CRITICA:** Il Comune di Monte Isola è stato oggetto di un **massiccio attacco informatico nel mese di gennaio 2025** che ha compromesso l'interezza dell'infrastruttura: client, server e backup. L'incidente ha dimostrato in modo inequivocabile che le misure di sicurezza esistenti erano **completamente inadeguate e inefficaci** nel proteggere l'ente da minacce cyber moderne.

Questo evento rappresenta il principale driver del presente progetto di revamp e sottolinea l'urgenza degli interventi proposti

### 2.3 Criticità Identificate

L'analisi dell'infrastruttura esistente, confermata drammaticamente dall'incidente di gennaio 2025, ha evidenziato le seguenti criticità, ordinate per livello di priorità:

#	Ambito	Criticità	Rischio	Priorità
1	Server/Endpoint	Server/Client non protetti da EDR	Nessuna capacità di rilevamento malware avanzato	Critica
2	Server	Sistemi operativi server in EOL (2008 R2)	Vulnerabilità note non patchabili, no supporto Microsoft	Critica
3	Server/Endpoint	Nessuna politica di patching	Vulnerabilità note sfruttabili dagli attaccanti	Critica



4	Rete	Firewall inefficace	Protezione perimetrale insufficiente	Critica
5	Rete	Nessuna segmentazione della rete	Propagazione laterale immediata delle minacce	Critica
6	Rete	Rete di backup non isolata/segregata	Backup compromessi insieme ai dati primari	Critica
7	Identità	Nessun MFA per posta e servizi	Accesso con sole credenziali rubabili	Critica
8	Backup	Assenza backup cloud/offline/immutabile	Perdita totale dati in caso di ransomware	Critica
9	Backup	Backup sulla stessa rete dei dati	Backup cifrati/cancellati insieme ai dati	Critica
10	Endpoint	Nessuna gestione centralizzata dei client	Impossibilità di applicare policy di sicurezza uniformi	Alta
11	Server	Mancanza di antispam	Email di phishing non filtrate	Alta
12	Identità	Nessuna policy di rotazione credenziali	Credenziali compromesse utilizzabili indefinitamente	Alta
13	Identità	Nessun monitoraggio degli accessi	Impossibilità di rilevare accessi anomali/malevoli	Alta
14	Servizi	Posta su provider tradizionale	Limitata resilienza, sicurezza e funzionalità	Media

#### Riepilogo per ambito:

Ambito	Critiche	Alte	Medie	Totale
Endpoint	3	1	-	4
Server	3	-	-	-
Rete	3	1	-	4
Identità	1	2	-	3
Backup	2	-	-	2
Servizi	-	-	1	1
<b>Totale</b>	<b>9</b>	<b>4</b>	<b>1</b>	<b>14</b>

#### Sintesi Impatto Incidente Gennaio 2025

L'attacco subito ha sfruttato simultaneamente molte delle vulnerabilità sopra elencate, dimostrando come la mancanza di un approccio di sicurezza strutturato esponga l'ente a rischi inaccettabili:

- **Assenza EDR:** il malware non è stato rilevato né bloccato
- **Rete non segmentata:** la minaccia si è propagata a tutti i sistemi senza ostacoli
- **Backup non isolati:** i backup sono stati compromessi insieme ai dati primari
- **Nessun MFA:** le credenziali compromesse hanno consentito accesso ai sistemi
- **Nessun monitoraggio:** l'attacco non è stato rilevato tempestivamente

#### 2.4 Obiettivi di Progetto

Alla luce dell'incidente subito e delle criticità identificate, gli obiettivi del progetto assumono carattere di urgenza:

1. **Mettere in sicurezza** la rete e i server/endpoint secondo le best practice
2. **Migrare** i servizi core (posta, file) verso soluzioni cloud affidabili
3. **Modernizzare** l'infrastruttura server con migrazione in datacenter
4. **Garantire** la conformità alle normative AGID e GDPR

## 5. Implementare una strategia di backup e continuità operativa

### 3. PERIMETRO DI PROGETTO

La definizione chiara del perimetro di progetto è un elemento essenziale per il successo dell'iniziativa. Stabilire con precisione cosa è incluso (in scope) e cosa è escluso (out of scope) permette di evitare ambiguità, gestire correttamente le aspettative degli stakeholder e mantenere il controllo su tempi e costi.

Il perimetro è stato definito attraverso un processo di analisi che ha considerato: - Le **priorità di sicurezza**: gli interventi che mitigano i rischi più elevati hanno precedenza - La **fattibilità tecnica**: gli interventi devono essere realizzabili senza stravolgere l'operatività quotidiana - Il **rapporto costo/beneficio**: gli investimenti devono produrre un valore tangibile per l'ente - Le **dipendenze esterne**: alcuni elementi dipendono da fornitori terzi e sono quindi gestiti separatamente

Di seguito il dettaglio delle sedi coinvolte, degli elementi inclusi nel progetto e di quelli esplicitamente esclusi.

#### 3.1 Sedi Coinvolte

Sede	Tipologia	Utenti	Connettività
Municipio	Principale	~12	FTTH INTRED
Biblioteca	Secondaria	2	FTTH INTRED
Infopoint	Secondaria	1	FTTH INTRED

#### 3.2 In Scope

Componente	Descrizione
Firewall	4 unità Fortinet (HA al Municipio) con SD-WAN
Switch	6 unità FortiSwitch PoE gestiti
Access Point	6 unità FortiAP con 3 SSID segregati
EDR/XDR	SentinelOne Complete su endpoint e server
Microsoft 365	Migrazione posta e dati (17 mailbox)
Backup M365	Acronis Cyber Protect SaaS
Domain Controller	Migrazione in datacenter Brescia
Collegamento stampanti	Integrazione in rete (apparati gestiti da terzi)

#### 3.3 Out of Scope

Componente	Motivazione
Cablaggio strutturato	Esistente e funzionale
UPS	Server locale sarà dismesso a regime
Stampanti	Gestite da altro fornitore
Telefonia	Valutazione futura
Videosorveglianza	Rete dedicata, altro appaltatore
Dispositivi mobili	Solo PC Windows in scope



SIEM	Non conveniente per dimensione ente
------	-------------------------------------

### 3.4 Punti di Attenzione

Punto	Descrizione	Mitigazione
Stampanti ad impatto	Ufficio Anagrafe, critiche per documenti	Sconsigliata soluzione thin client
Applicativi legacy	Dipendenza da server locale	Fase transitoria dedicata

## 4. ARCHITETTURA DI RETE

L'architettura di rete costituisce le fondamenta su cui poggia l'intera infrastruttura IT. Una rete ben progettata non è solo un mezzo per connettere dispositivi, ma rappresenta il primo livello di difesa contro le minacce informatiche e il fattore abilitante per tutti i servizi digitali dell'ente.

Il progetto prevede una riprogettazione completa dell'infrastruttura di rete del Comune, passando da una rete "piatta" e non gestita a un'architettura moderna caratterizzata da:

- **Connettività ad alta velocità:** fibra ottica FTTH in tutte le sedi, in sostituzione delle connessioni precedenti
- **Interconnessione sicura:** tecnologia SD-WAN per collegare le tre sedi attraverso tunnel cifrati su internet, eliminando la necessità di costose linee dedicate
- **Gestione centralizzata:** tutti gli apparati (firewall, switch, access point) sono dello stesso vendor e gestibili da un'unica console, riducendo la complessità operativa
- **Segmentazione avanzata:** suddivisione della rete in VLAN funzionali per isolare il traffico e contenere eventuali incidenti di sicurezza
- **Ridondanza:** configurazione in alta disponibilità (HA) nella sede principale per garantire continuità di servizio

La scelta di una piattaforma Fortinet integrata (Security Fabric) permette di ottenere visibilità completa sul traffico di rete, correlazione degli eventi di sicurezza tra i diversi componenti e risposta coordinata alle minacce.

### 4.1 Connettività WAN

Voce	Dettaglio
Provider	INTRED
Tecnologia	FTTH (Fiber To The Home)
Copertura	Tutte e 3 le sedi

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





Interconnessione	SD-WAN su firewall Fortinet
------------------	-----------------------------

La connettività WAN è oggetto di un progetto separato, già in fase di esecuzione. Il Comune di Monte Isola ha recentemente stipulato un accordo con il provider **INTRED S.p.A.** per portare connettività in fibra ottica (FTTH) a tutte le sedi comunali. Questo intervento infrastrutturale rappresenta un prerequisito fondamentale per l'implementazione dell'architettura SD-WAN descritta nel presente documento e garantirà banda simmetrica ad alta velocità, bassa latenza e affidabilità di connessione necessarie per supportare i servizi cloud e l'interconnessione sicura tra le sedi.

#### 4.1.1 Requisiti Infrastrutturali per SD-WAN

Per il corretto funzionamento dell'architettura SD-WAN e per garantire affidabilità e continuità operativa, ogni sede deve soddisfare i seguenti requisiti infrastrutturali:

##### Requisiti Connettività:

Requisito	Specifica	Motivazione
Tecnologia	FTTH (Fiber To The Home)	Banda garantita e bassa latenza per SD-WAN
Subnet pubblica	/30 di consegna	Indirizzamento IP pubblico per terminazione tunnel
Consegna fisica	Doppia porta Ethernet ridondata (bridge)	Per apparati HA attivo/passivo

##### Requisiti Rack e Alimentazione:

Requisito	Specifica	Motivazione
Spazio rack	Minimo 1 RU per armadio rack	Installazione apparati firewall
PDU	Minimo 2 PDU per rack	Alimentazione ridondata firewall (doppio alimentatore)
UPS	Consigliato UPS a rack	Continuità operativa firewall in caso di interruzione elettrica

**Note:** - La doppia porta Ethernet in configurazione bridge sul punto di consegna INTRED consente di collegare entrambi i firewall in HA (sede Municipio) o di avere ridondanza sul collegamento fisico - La presenza di 2 PDU separate permette di alimentare i due alimentatori del firewall da circuiti distinti, aumentando la resilienza - L'UPS a rack è fortemente consigliato per garantire che i firewall rimangano operativi durante brevi interruzioni elettriche, mantenendo attiva la connettività SD-WAN e i servizi di sicurezza

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it







#### Riepilogo Requisiti per Sede:

Sede	FTTH + /30	Doppia ETH	1 RU	2 PDU	UPS (cons.)
Municipio	✓	✓	✓	✓	✓
Biblioteca	✓	✓	✓	✓	✓
Infopoint	✓	✓	✓	✓	✓

#### 4.2 Criticità della Connettività e Raccomandazione Backup

Con la migrazione dei servizi core verso il cloud (Microsoft 365, SaaS) e lo spostamento del Domain Controller in un datacenter remoto, la **connettività Internet assume un ruolo critico e strategico** per la continuità operativa dell'ente. Un'interruzione della linea principale comporterebbe oggi il blocco quasi totale delle attività amministrative.

Considerata la natura geografica di Monte Isola e la dipendenza da un unico media trasmissivo (fibra ottica), si **raccomanda fortemente** che la sede del **Municipio sia dotata di una connettività secondaria di backup** su media trasmissivo differente dalla fibra (es. FWA, LTE/5G o Starlink). Questa linea di backup garantirà l'operatività e l'accesso ai servizi critici anche in caso di guasto o interruzione della connettività primaria, assicurando la Business Continuity dell'ente.

#### 4.3 Apparati di Rete

Tipologia	Modello	Quantità	Sede	Note
Firewall	FortiGate 50G	2	Municipio	High Availability (Active-Passive)
Firewall	FortiGate 40F	1	Biblioteca	Standalone
Firewall	FortiGate 40F	1	Infopoint	Standalone

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





Switch	FortiSwitch FS-148F-PoE	2	Municipio	48 porte PoE+
Switch	FortiSwitch FS-124F-PoE	1	Biblioteca	24 porte PoE+
Switch	FortiSwitch FS-108F-PoE	3	Infopoint	8 porte PoE+
Access Point	FortiAP 231K	3	Municipio	WiFi 7 (802.11be)
Access Point	FortiAP 231K	1	Biblioteca	WiFi 7 (802.11be)
Access Point	FortiAP 231K	2	Infopoint	WiFi 7 (802.11be)

#### Riepilogo per sede:

Sede	Firewall	Switch	Access Point	Totale apparati
Municipio	2	2	3	7
Biblioteca	1	1	1	3
Infopoint	1	3	2	6
<b>Totale</b>	<b>4</b>	<b>6</b>	<b>6</b>	<b>16</b>

#### 4.3.1 Funzionalità Firewall

I firewall FortiGate sono configurati con le seguenti funzionalità:

- Next-Generation Firewall (NGFW)
- SD-WAN per interconnessione sedi
- VPN IPSec site-to-site
- Web Filtering

#### TIER 1 srl

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





- Application Control
- Intrusion Prevention System (IPS)
- Antivirus perimetrale
- SSL Inspection

#### 4.3.2 Caratteristiche Switch

I FortiSwitch offrono le seguenti funzionalità:

- Power over Ethernet (PoE+) per alimentazione AP e telefoni
- Gestione centralizzata da FortiGate
- Supporto VLAN 802.1Q
- Network Access Control (NAC)

#### 4.3.3 Gestione Access Point

Gli Access Point FortiAP 231K supportano WiFi 7 (802.11be) e sono gestiti tramite il controller integrato nei FortiGate, garantendo configurazione centralizzata e policy di sicurezza uniformi su tutte le sedi.

#### 4.3.4 Client e Postazioni di Lavoro

L'analisi dell'infrastruttura client esistente ha evidenziato una situazione complessivamente positiva: la quasi totalità delle postazioni di lavoro è dotata di sistema operativo **Windows 11 Pro**, con sole due eccezioni. Questo scenario indica che il parco macchine è relativamente recente e conforme ai requisiti hardware e software necessari per le attività d'ufficio e per l'utilizzo dei servizi cloud Microsoft 365.

Voce	Dettaglio
Sistema Operativo	Windows 11 Pro
Postazioni conformi	~13 su 15
Postazioni da valutare	2
Interventi hardware	Non previsti

#### Valutazione:

La maggior parte dei client risulta idonea al lavoro di ufficio e **non necessita di interventi a livello hardware o di sistema operativo**. Le due postazioni non conformi saranno oggetto di valutazione specifica per determinare se sia necessario un upgrade o una sostituzione.

#### TIER 1 srl

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





#### Interventi previsti:

Non sono previsti interventi strutturali significativi sulla componente client. L'attenzione sarà invece focalizzata sul rafforzamento dei processi di:

- **Protezione:** deployment dell'agente EDR SentinelOne su tutte le postazioni
- **Aggiornamento:** implementazione di policy centralizzate per Windows Update e patch management
- **Mantenimento:** configurazione di strumenti MDM per inventario, monitoraggio e gestione remota
- **Hardening:** applicazione di baseline di sicurezza e policy di gruppo (GPO) tramite Active Directory

Questo approccio consente di massimizzare il ritorno sull'investimento esistente, evitando spese non necessarie per hardware già adeguato, e concentrando le risorse sugli aspetti di sicurezza e gestione che rappresentano le reali criticità emerse dall'analisi.

#### 4.4 Schema VLAN

Convenzione di Naming

VLAN ID	Nome	Funzione	Accesso
1	LAN	Rete principale	Client, stampanti, server
10	WiFi-Office	Dispositivi comunali wireless	Accesso completo LAN
20	WiFi-Mobile	Dispositivi privati dipendenti	Solo internet
30	WiFi-Ospiti	Rete guest	Solo internet, client isolation
99	Management	Gestione apparati	Solo IT autorizzato

##### 4.4.1 Indirizzamento IP per Sede

Municipio (192.168.20x.0/24)

VLAN	Subnet	Gateway	DHCP Range
1 - LAN	192.168.205.0/24	192.168.205.1	.100-.200
10 - WiFi-Office	192.168.201.0/24	192.168.201.1	.100-.200

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





20 - WiFi-Mobile	192.168.202.0/24	192.168.202.1	.100-.200
30 - WiFi-Ospiti	192.168.203.0/24	192.168.203.1	.100-.200
99 - Management	192.168.209.0/24	192.168.209.1	Statico

#### Biblioteca (192.168.19x.0/24)

VLAN	Subnet	Gateway	DHCP Range
1 - LAN	192.168.195.0/24	192.168.195.1	.100-.200
10 - WiFi-Office	192.168.191.0/24	192.168.191.1	.100-.200
20 - WiFi-Mobile	192.168.192.0/24	192.168.192.1	.100-.200
30 - WiFi-Ospiti	192.168.193.0/24	192.168.193.1	.100-.200
99 - Management	192.168.199.0/24	192.168.199.1	Statico

#### Infopoint (192.168.18x.0/24)

VLAN	Subnet	Gateway	DHCP Range
1 - LAN	192.168.185.0/24	192.168.185.1	.100-.200
10 - WiFi-Office	192.168.181.0/24	192.168.181.1	.100-.200
20 - WiFi-Mobile	192.168.182.0/24	192.168.182.1	.100-.200
30 - WiFi-Ospiti	192.168.183.0/24	192.168.183.1	.100-.200
99 - Management	192.168.189.0/24	192.168.189.1	Statico

#### TIER 1 srl

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





## 4.5 Inter-VLAN Routing e Segregazione della Rete

### Architettura di Routing

L'architettura di rete adottata implementa il modello a **singolo gateway centralizzato**, nel quale il firewall FortiGate funge da unico punto di routing tra tutte le VLAN. In questa configurazione, gli switch FortiSwitch operano esclusivamente a Layer 2 (switching), mentre tutte le funzioni di Layer 3 (routing) sono centralizzate sul firewall. Ogni VLAN è configurata come interfaccia virtuale sul FortiGate, che ne gestisce il gateway predefinito.

Questa scelta architettureale, pur introducendo un potenziale collo di bottiglia sul firewall, offre vantaggi significativi in termini di sicurezza:

- **Ispezione completa del traffico:** ogni pacchetto che transita tra VLAN diverse attraversa necessariamente il firewall, dove viene sottoposto a ispezione stateful, analisi applicativa (Layer 7) e verifica contro le policy di sicurezza
- **Visibilità centralizzata:** tutto il traffico inter-VLAN è visibile, loggabile e analizzabile da un unico punto, semplificando il monitoraggio e l'incident response
- **Policy enforcement granulare:** le regole di accesso tra segmenti di rete sono definite e applicate centralmente sul firewall, garantendo coerenza e facilità di gestione
- **Prevenzione del lateral movement:** un eventuale attaccante che compromette un dispositivo in una VLAN non può raggiungere altre VLAN senza attraversare il firewall, che può rilevare e bloccare tentativi di movimento laterale

### 4.5.1 PRINCIPIO DI SEGREGAZIONE

La segregazione della rete interna si basa sul principio **"default deny"**: per impostazione predefinita, il traffico tra VLAN diverse è bloccato. Solo i flussi esplicitamente autorizzati e necessari per l'operatività sono consentiti. Questo approccio, noto come **"Zero Trust Network"**, assume che nessun segmento di rete sia intrinsecamente affidabile e richiede una validazione esplicita per ogni comunicazione.

In pratica, la segmentazione implementata crea i seguenti **domini di sicurezza**:

Dominio	VLAN	Livello di trust	Accesso consentito
Produzione	VLAN 1 (LAN)	Alto	Internet, altre sedi, DC
WiFi Aziendale	VLAN 10 (Office)	Medio-Alto	LAN locale, Internet
BYOD	VLAN 20 (Mobile)	Basso	Solo Internet
Guest	VLAN 30 (Ospiti)	Nessuno	Solo Internet, isolamento client
Management	VLAN 99	Critico	Accesso solo da IT autorizzato

## 4.5.2 MATRICE DELLE POLICY INTER-VLAN

Sorgente	Destinazione	Azione	Giustificazione
VLAN 1 (LAN)	Internet	ALLOW	Navigazione e servizi cloud
VLAN 1 (LAN)	VLAN 1 altre sedi	ALLOW	Comunicazione inter-sede via SD-WAN
VLAN 10 (Office)	VLAN 1	ALLOW	Accesso risorse LAN
VLAN 20 (Mobile)	Internet	ALLOW	Solo navigazione
VLAN 20 (Mobile)	Tutte le VLAN	DENY	Segregazione completa
VLAN 30 (Ospiti)	Internet	ALLOW	Solo navigazione
VLAN 30 (Ospiti)	Tutte le VLAN	DENY	Segregazione completa
VLAN 99 (Mgmt)	Tutte le VLAN	ALLOW	Gestione apparati
Tutte le VLAN	VLAN 99 (Mgmt)	DENY	Protezione piano di management

Nota: l'accesso da VLAN 10 (Office) verso VLAN 1 (LAN) sarà consentito solo per servizi autorizzati (es. stampa, DNS, SMB/HTTP verso applicativi interni) tramite ACL puntuali; il resto del traffico resta in deny (principio default deny).

## SICUREZZA

### 5.1 Network Security

La sicurezza della rete rappresenta il primo e fondamentale livello di difesa dell'infrastruttura IT del Comune. In un contesto in cui le minacce informatiche sono in costante evoluzione e gli enti pubblici rappresentano obiettivi sempre più frequenti di attacchi cyber, è essenziale implementare un'architettura di sicurezza multilivello che protegga il perimetro, segmenti il traffico interno e garantisca visibilità completa sulle comunicazioni.

L'approccio adottato si basa sul principio di **"Defense in Depth"** (difesa in profondità), che prevede molteplici barriere di sicurezza sovrapposte: protezione perimetrale tramite firewall Next-Generation, segmentazione della rete attraverso VLAN dedicate per funzione, e



controllo granulare degli accessi tra i diversi segmenti. Questa strategia garantisce che, anche in caso di compromissione di un singolo elemento, la propagazione della minaccia sia contenuta e l'impatto sull'operatività dell'ente sia minimizzato.

La scelta di una piattaforma unificata Fortinet (firewall, switch, access point) consente inoltre una gestione centralizzata e coerente delle policy di sicurezza, riducendo la complessità operativa e migliorando i tempi di risposta agli incidenti.

### 5.1.1 Protezione Perimetrale

La protezione perimetrale è garantita dai firewall FortiGate con licenza **UTP (Unified Threat Protection)**, un bundle completo di servizi di sicurezza che trasforma il firewall da semplice filtro di pacchetti a piattaforma di protezione avanzata multi-layer. La licenza UTP include tutti i servizi di sicurezza necessari per una protezione enterprise-grade, con aggiornamenti continui delle signature e dei database di threat intelligence direttamente dai FortiGuard Labs, il centro di ricerca Fortinet che analizza miliardi di eventi di sicurezza quotidianamente a livello globale.

**Intrusion Prevention System (IPS):** Il sistema di prevenzione delle intrusioni analizza in tempo reale tutto il traffico di rete alla ricerca di pattern di attacco noti e comportamenti anomali. L'IPS FortiGate utilizza un database di oltre 10.000 signature costantemente aggiornate che identificano exploit, vulnerabilità note (CVE), tentativi di buffer overflow, SQL injection, command injection e altre tecniche di attacco. Quando viene rilevato un tentativo di intrusione, il sistema può bloccare automaticamente il traffico malevolo, generare un alert e loggare l'evento per successive analisi forensi. Questa protezione è fondamentale per difendersi da attacchi che sfruttano vulnerabilità nei sistemi esposti, anche prima che le patch siano disponibili o applicate.

**Antivirus Gateway:** La scansione antivirus perimetrale ispeziona tutti i file che transitano attraverso il firewall — download web, allegati email, trasferimenti FTP — prima che raggiungano gli endpoint interni. A differenza dell'antivirus installato sul PC, che interviene quando il file è già sul dispositivo, l'antivirus gateway blocca le minacce al confine della rete, impedendo che il malware entri nell'infrastruttura. Il motore antivirus FortiGate combina signature tradizionali con tecniche euristiche e machine learning per identificare anche varianti sconosciute di malware. La scansione avviene in streaming per minimizzare la latenza percepita dagli utenti.

**Web Filtering:** Il servizio di filtraggio web categorizza e controlla l'accesso ai siti internet in base a oltre 90 categorie predefinite (malware, phishing, gambling, adult content, social media, streaming, ecc.). FortiGuard mantiene un database di miliardi di URL categorizzati, aggiornato in tempo reale man mano che nuovi siti vengono analizzati. Oltre a bloccare l'accesso a siti notoriamente malevoli (distribuzione malware, phishing, command & control), il web filtering consente di definire policy di navigazione che limitano l'accesso a categorie di siti non pertinenti all'attività lavorativa, migliorando la produttività e riducendo il consumo di banda. Per il Comune, verranno configurate policy che bloccano automaticamente siti pericolosi e consentono di gestire l'accesso a categorie discrezionali.

**Application Control:** Il controllo applicativo opera a Layer 7 dello stack di rete, identificando e gestendo le applicazioni indipendentemente dalla porta o dal protocollo utilizzato. Mentre un firewall tradizionale può solo bloccare o permettere traffico su determinate porte (es. porta 443 per HTTPS), l'Application Control riconosce le applicazioni specifiche che utilizzano quella porta — distinguendo, ad esempio, tra navigazione web legittima, Dropbox, BitTorrent o una sessione di desktop remoto mascherata. Questo consente di applicare policy granulari: permettere Microsoft Teams ma bloccare WhatsApp Web, consentire YouTube in modalità educational ma bloccare lo streaming video generico. FortiGate riconosce oltre 4.000 applicazioni e protocolli, con aggiornamenti settimanali per includere nuove applicazioni.

**FortiSandbox Cloud:** La sandbox cloud rappresenta l'ultima linea di difesa contro le minacce sconosciute (zero-day). Quando un file sospetto non viene riconosciuto dai motori antivirus tradizionali — perché nuovo, offuscato o specificamente creato per eludere le signature — viene automaticamente inviato alla FortiSandbox Cloud per un'analisi comportamentale approfondita. Il file viene eseguito in un ambiente virtuale isolato dove il sistema osserva il suo comportamento: tenta di modificare il registro di sistema? Cerca di connettersi a server esterni? Cifra file? Installa backdoor? Questa analisi dinamica permette di identificare malware che non ha ancora una signature nota. Se il comportamento risulta malevolo, il file viene bloccato e la signature viene distribuita globalmente a tutti i dispositivi Fortinet, proteggendo l'intera community di clienti dalla nuova minaccia.

### 5.1.2 Accesso remoto utenti e fornitori

L'accesso remoto sarà erogato tramite VPN SSL/IPSec sui FortiGate, con autenticazione federata a Entra ID e MFA obbligatoria. Sono previsti profili separati per utenti interni e fornitori/MSP, con privilegi minimi necessari. Tutte le sessioni sono loggiate su FortiCloud; le credenziali privilegiate seguono il principio di least privilege e vengono abilitate solo per la finestra di intervento.

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it







### 5.1.3 Segmentazione di Rete

La segmentazione della rete tramite VLAN (Virtual Local Area Network) rappresenta una delle misure di sicurezza più efficaci e al contempo più sottovalutate nelle infrastrutture IT. In una rete “piatta”, priva di segmentazione, un attaccante che riesca a compromettere un singolo dispositivo può muoversi lateralmente senza ostacoli, raggiungendo rapidamente sistemi critici, server e dati sensibili. Questo scenario, noto come “lateral movement”, è alla base della maggior parte degli attacchi ransomware che hanno colpito enti pubblici e aziende negli ultimi anni.

L’implementazione di VLAN dedicate per funzione consente di creare **compartimenti stagni** all’interno della rete: i dispositivi della rete ospiti non possono comunicare con i PC degli uffici, i dispositivi personali dei dipendenti sono isolati dalle risorse comunali, e gli apparati di rete sono protetti in un segmento di management accessibile solo al personale IT autorizzato. Ogni comunicazione tra VLAN diverse deve transitare attraverso il firewall, dove viene ispezionata e autorizzata secondo policy predefinite.

Questo approccio offre molteplici vantaggi:

- **Contenimento delle minacce:** in caso di infezione malware, la propagazione è limitata al solo segmento compromesso
- **Riduzione della superficie di attacco:** i servizi critici non sono raggiungibili da reti non autorizzate
- **Conformità normativa:** la segregazione dei dati è un requisito esplicito delle misure minime AGID e del GDPR
- **Visibilità e controllo:** tutto il traffico inter-VLAN è loggato e analizzabile per audit e incident response
- **Gestione semplificata:** le policy di sicurezza possono essere applicate per segmento anziché per singolo dispositivo

Nel contesto del Comune di Monte Isola, la segmentazione in 5 VLAN per sede (LAN, WiFi Office, WiFi Mobile, WiFi Ospiti, Management) garantisce che anche in presenza di utenti esterni (cittadini, visitatori) connessi alla rete WiFi guest, le risorse comunali rimangano completamente inaccessibili e protette.

### 5.2 Endpoint Security

La protezione degli endpoint rappresenta oggi la linea di difesa più critica in qualsiasi strategia di cybersecurity. Gli endpoint/PC, laptop e server, sono il punto di ingresso privilegiato per la maggior parte degli attacchi informatici: phishing, malware, ransomware e attacchi mirati colpiscono quasi sempre l’utente finale prima di propagarsi all’interno dell’infrastruttura.

I tradizionali software antivirus, basati esclusivamente su firme e database di minacce conosciute, non sono più sufficienti a fronteggiare il panorama delle minacce moderne. Gli attacchi odierni utilizzano tecniche avanzate di evasione, malware polimorfo, exploit zero-day e tecniche “fileless” che operano interamente in memoria senza lasciare tracce sul disco. Per contrastare queste minacce è necessario adottare soluzioni di nuova generazione denominate **EDR (Endpoint Detection and Response)**.

A differenza degli antivirus tradizionali, le soluzioni EDR:

- **Analizzano i comportamenti** anziché cercare solo firme note, identificando attività sospette anche da minacce mai viste prima
- **Forniscono visibilità completa** su ogni processo, connessione di rete e modifica al sistema operativo
- **Consentono risposta rapida** con capacità di isolamento automatico dell’endpoint compromesso dalla rete
- **Registrano una timeline forense** di tutte le attività, fondamentale per l’analisi post-incidente
- **Integrano capacità di remediation** incluso, in alcuni casi, il rollback delle modifiche apportate da ransomware

Per il Comune di Monte Isola, la protezione degli endpoint assume particolare rilevanza considerando la natura dei dati trattati (dati personali dei cittadini, dati dell’anagrafe, informazioni finanziarie) e gli obblighi normativi derivanti dal GDPR e dalle misure minime AGID.

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





### 5.2.1 Soluzione EDR/XDR

Voce	Dettaglio
Prodotto	SentinelOne Complete
Tipologia	EDR/XDR
Copertura Endpoint	~15 workstation Windows
Copertura Server	Server fisici legacy + futuri server datacenter

SentinelOne Complete è una piattaforma EDR/XDR di ultima generazione, riconosciuta come leader nel Gartner Magic Quadrant per le soluzioni di Endpoint Protection. La caratteristica distintiva di SentinelOne è la sua architettura **autonoma**: l'agente installato sull'endpoint è in grado di rilevare, bloccare e remediare le minacce in tempo reale, senza necessità di connessione al cloud o intervento umano. Questo è particolarmente importante per garantire protezione anche in caso di interruzione della connettività.

**Funzionalità principali:** - **Prevention:** Blocco minacce note e zero-day tramite motori AI/ML che analizzano il comportamento dei processi - **Detection:** Rilevamento di comportamenti anomali, tecniche di attacco (MITRE ATT&CK) e indicatori di compromissione - **Response:** Risposta automatica con isolamento dell'endpoint dalla rete, kill dei processi malevoli e quarantena dei file - **Hunting:** Strumenti di threat hunting per ricerca proattiva di minacce nascoste nell'infrastruttura - **Rollback:** Capacità unica di ripristino automatico da ransomware, annullando le modifiche ai file cifrati

### 5.2.2 Mobile Device Management (MDM)

Implementazione di soluzione MDM per: Inventario centralizzato dispositivi, Distribuzione patch di sicurezza, Enforcement policy di sicurezza, Gestione configurazioni Windows

## 5.3 Identity Security

Nel panorama attuale delle minacce informatiche, l'identità digitale è diventata il nuovo perimetro di sicurezza. Con la migrazione dei servizi in cloud e l'adozione di modelli di lavoro flessibili, il tradizionale concetto di "proteggere il perimetro della rete" non è più sufficiente: gli utenti accedono ai dati aziendali da qualsiasi luogo e dispositivo, rendendo le credenziali di accesso il bersaglio principale degli attaccanti.

Le statistiche sono eloquenti: oltre l'80% delle violazioni di dati coinvolge credenziali compromesse. Gli attacchi di phishing, il credential stuffing (utilizzo di credenziali rubate da altri servizi) e il password spraying sono tecniche quotidianamente utilizzate contro organizzazioni di ogni dimensione. Per una Pubblica Amministrazione, la compromissione di un account può significare accesso non autorizzato a dati personali dei cittadini, con conseguenze gravissime in termini di violazione GDPR e danno reputazionale.

La strategia di Identity Security del progetto si basa sul principio "**Zero Trust**": non fidarsi mai, verificare sempre. Ogni accesso viene valutato in base a molteplici fattori (identità dell'utente, stato del dispositivo, località, comportamento) e l'autenticazione a più fattori diventa obbligatoria per tutti gli utenti senza eccezioni.

### 5.3.1 Multi-Factor Authentication (MFA)

L'autenticazione a più fattori (MFA) è la misura di sicurezza più efficace contro il furto di credenziali. Richiedendo un secondo fattore di autenticazione oltre alla password, MFA rende inutili le credenziali rubate: anche se un attaccante conosce la password, non può accedere senza il secondo fattore (tipicamente un codice generato dall'app Microsoft Authenticator sullo smartphone dell'utente).

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





Implementazione **obbligatoria** di MFA per tutti gli account Microsoft 365: Protezione da compromissione credenziali, secondo fattore via app authenticator o SMS, applicazione a tutti gli utenti senza eccezioni

### 5.3.2 Conditional Access

Configurazione policy di accesso condizionale tramite Entra ID P2:

Policy	Descrizione
Geo-blocking	Blocco accessi da paesi non autorizzati
Device compliance	Accesso solo da dispositivi conformi
Risk-based access	Analisi rischio sign-in in tempo reale
Session controls	Limitazione sessioni e timeout

### 5.3.3 Patch Management e hardening

- **Endpoint/OS/terze parti:** patching automatizzato tramite RMM gestito dal MSP con finestre serali/mensili; approvazione modifiche critiche concordata con il Comune.
- **Firmware security/network:** aggiornamenti Fortinet pianificati dal MSP con finestre di manutenzione definite e procedure di rollback.
- **Responsabilità:** MSP esegue monitoraggio, testing e deployment; il Comune approva le finestre che impattano il servizio. Baseline di hardening applicate via GPO/MDM ove applicabile.

## SERVIZI CLOUD E MICROSOFT 365

### 6.1 Perché Microsoft 365: Vantaggi rispetto alle Soluzioni Tradizionali

La migrazione da una soluzione di posta elettronica tradizionale come Aruba a Microsoft 365 rappresenta un salto qualitativo significativo che va ben oltre il semplice cambio di provider email. Microsoft 365 è una piattaforma integrata di produttività e collaborazione che trasforma il modo in cui un'organizzazione lavora, comunica e protegge i propri dati.

#### 6.1.1 Limiti delle Soluzioni Tradizionali (Aruba e similari)

Le soluzioni di posta tradizionali, pur essendo funzionali per l'invio e la ricezione di email, presentano limitazioni strutturali che le rendono inadeguate alle esigenze moderne di una Pubblica Amministrazione:

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





Aspetto	Soluzione Tradizionale (Aruba)	Limitazione
Funzionalità	Solo email e (opzionalmente) PEC	Nessuno strumento di collaborazione integrato
Storage	Spazio limitato per casella	Gestione manuale dello spazio, rischio perdita email
Accesso	Webmail base o client desktop	Esperienza utente limitata, scarsa mobilità
Collaborazione	Assente	Necessità di strumenti terzi per condivisione documenti
Sicurezza	Antispam/Antivirus base	Nessuna protezione avanzata contro phishing mirato
Compliance	Limitata	Strumenti di audit e retention basilari
Disponibilità	SLA standard	Nessuna ridondanza geografica garantita

#### 6.1.2 Vantaggi di Microsoft 365

Funzionalità e Produttività

Microsoft 365 Business Standard include un ecosistema completo di strumenti integrati:

Componente	Funzionalità	Valore per il Comune
Exchange Online	Email professionale con 50 GB per casella	Spazio abbondante, nessuna gestione manuale
Microsoft Teams	Chat, videochiamate, riunioni online	Collaborazione tra sedi, smart working, riunioni con cittadini
SharePoint Online	Intranet e gestione documentale	Repository centralizzato documenti comunali
OneDrive for Business	1 TB storage cloud per utente	Backup automatico documenti, accesso ovunque

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





Office Online	Word, Excel, PowerPoint nel browser	Modifica documenti senza installazione software
Office Desktop Apps	Suite Office completa installabile	Produttività avanzata su PC
Microsoft Planner	Gestione attività e progetti	Coordinamento attività tra uffici
Microsoft Forms	Creazione questionari e moduli	Raccolta feedback cittadini, modulistica online

### 6.1.3 Sicurezza Integrata

Microsoft 365 include funzionalità di sicurezza enterprise che sarebbero impossibili da ottenere con soluzioni tradizionali:

Funzionalità	Descrizione	Protezione
Exchange Online Protection (EOP)	Filtraggio email incluso in ogni licenza	Anti-malware, anti-spam, anti-phishing base
Safe Attachments	Analisi allegati in sandbox	Blocco malware zero-day negli allegati
Safe Links	Verifica URL in tempo reale	Protezione da link malevoli anche post-consegna
Anti-Phishing AI	Machine learning anti-impersonation	Rilevamento tentativi di frode e CEO fraud
Data Loss Prevention (DLP)	Policy prevenzione fuga dati	Blocco invio dati sensibili all'esterno
Message Encryption	Crittografia email	Comunicazioni riservate con esterni
Audit Logging	Log completi attività utenti	Tracciabilità per compliance e incident response

Con l'aggiunta di **Microsoft Defender for Office365 P1** (incluso nel progetto), la protezione si estende ulteriormente con: - Protezione avanzata e integrata con la console M365 - Rilevamento e risposta automatica alle minacce - Dashboard unificata per la gestione della sicurezza

### 6.1.4 Identity e Access Management

La licenza **Entra ID P2** (già Microsoft Azure AD P2) inclusa nel progetto abilita funzionalità di sicurezza dell'identità di livello enterprise:

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





Funzionalità	Descrizione	Beneficio
Multi-Factor Authentication (MFA)	Secondo fattore obbligatorio	Protezione da furto credenziali
Conditional Access	Policy di accesso contestuali	Accesso solo da dispositivi/luoghi sicuri
Identity Protection	Rilevamento rischi sign-in	Blocco automatico accessi sospetti
Privileged Identity Management (PIM)	Gestione accessi privilegiati	Elevazione temporanea privilegi admin
Access Reviews	Revisione periodica accessi	Rimozione automatica accessi obsoleti
Sign-in Risk Policies	Risposta automatica a rischi	Richiesta MFA aggiuntiva se rischio elevato

#### 6.1.5 Compliance e Conformità Normativa

Microsoft 365 è progettato per soddisfare i più stringenti requisiti normativi globali, un aspetto fondamentale per una Pubblica Amministrazione:

Certificazione/Standard	Descrizione	Rilevanza PA
ISO 27001	Sistema gestione sicurezza informazioni	Standard richiesto da AGID
ISO 27017	Controlli sicurezza servizi cloud	Specifico per cloud security
ISO 27018	Protezione dati personali nel cloud	Allineamento GDPR
SOC 1, SOC 2, SOC 3	Audit controlli interni	Garanzia processi sicuri
GDPR	Regolamento europeo privacy	Obbligatorio per PA italiana
Qualificazione ACN	Cloud marketplace italiano	Microsoft è CSP qualificato

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





**Data Residency:** Microsoft garantisce che i dati dei tenant europei risiedano in datacenter situati nell'Unione Europea (Paesi Bassi e Irlanda), soddisfacendo i requisiti di sovranità del dato previsti dalla normativa italiana ed europea.

Alta Disponibilità e Disaster Recovery

Aspetto	Microsoft 365	Soluzione Tradizionale
<b>SLA Uptime</b>	99,9% garantito contrattualmente	Variabile, spesso non garantito
<b>Ridondanza</b>	Geografica multi-datacenter	Singolo datacenter
<b>Backup infrastruttura</b>	Automatico e trasparente	A carico del cliente
<b>Disaster Recovery</b>	RTO/RPO in minuti	Ore o giorni
<b>Manutenzione</b>	Zero downtime (rolling updates)	Finestre di manutenzione

#### 6.1.6 Confronto Economico TCO

Oltre ai vantaggi funzionali, Microsoft 365 offre un Total Cost of Ownership (TCO) competitivo quando si considerano tutti i componenti:

Voce	Soluzione Tradizionale	Microsoft 365
Email hosting	✓ (costo base)	✓ Incluso
Antispam/Anti virus avanzato	Costo aggiuntivo	✓ Incluso
Suite Office licenze	Acquisto separato (~€300/utente)	✓ Incluso
Storage cloud	Servizio separato	✓ 1 TB/utente incluso
Videoconferenza	Servizio separato	✓ Teams incluso
Collaboration tools	Servizi separati	✓ SharePoint/Planner inclusi

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





MFA/Security avanzata	Non disponibile o costo extra	✓ Incluso (con Entra P2)
Compliance tools	Non disponibile	✓ Incluso

#### 6.1.7 Sintesi: Perché Microsoft 365 per il Comune di Monte Isola

La scelta di Microsoft 365 per il Comune di Monte Isola si basa su considerazioni strategiche concrete:

6. **Sicurezza enterprise-grade:** Protezione da minacce moderne (phishing, ransomware, data breach) con tecnologie AI che un piccolo ente non potrebbe permettersi autonomamente
7. **Compliance semplificata:** Certificazioni e strumenti di audit già inclusi, fondamentali per rispettare GDPR e direttive AGID senza investimenti aggiuntivi
8. **Continuità operativa garantita:** SLA 99,9% e infrastruttura ridondante eliminano il rischio di downtime prolungati
9. **Collaborazione moderna:** Possibilità di smart working, riunioni da remoto con cittadini, condivisione documenti sicura tra sedi
10. **Scalabilità:** Possibilità di aggiungere utenti e funzionalità senza interventi infrastrutturali
11. **Investimento nel futuro:** Piattaforma in continua evoluzione con nuove funzionalità (es. Copilot AI) incluse senza costi aggiuntivi
12. **Allineamento al Piano Triennale AGID:** Rispetto del principio “cloud first” per la Pubblica Amministrazione

## 6.2 Migrazione Posta Elettronica

La migrazione della posta elettronica da Aruba a Microsoft 365 rappresenta uno degli interventi più delicati del progetto, in quanto coinvolge direttamente tutti gli utenti e le comunicazioni quotidiane dell’ente. Una migrazione mal pianificata può causare perdita di email, interruzioni prolungate del servizio e disagi significativi per dipendenti e cittadini.

Per minimizzare i rischi e garantire una transizione fluida, è stata scelta la metodologia **Cutoff Migration** (migrazione con taglio netto), che prevede: - Preparazione completa dell’ambiente Microsoft 365 prima della migrazione - Migrazione effettiva dei dati in un’unica finestra temporale - Cambio immediato dei record DNS (MX) al termine della migrazione - Nessun periodo di coesistenza tra i due sistemi

### 6.2.1 Strategia di Migrazione

Voce	Dettaglio
Origine	Aruba
Destinazione	Microsoft 365 (Exchange Online)

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it







<b>Dominio</b>	comune.monteisola.bs.it
<b>Metodo</b>	Cutoff Migration
<b>Finestra temporale</b>	Weekend (sabato-domenica)
<b>Oggetti migrati</b>	Email, Calendari, Contatti

#### Perché Cutoff Migration nel Weekend:

La scelta di eseguire la migrazione durante il weekend è strategica per diversi motivi: **Minimizzazione del downtime percepito**: gli utenti non lavorano, quindi eventuali disservizi temporanei non impattano l'operatività, **Tempo sufficiente per la migrazione**: 48 ore consentono di completare il trasferimento di tutti i dati con margine per imprevisti, **Possibilità di rollback**: in caso di problemi critici, c'è tempo per tornare alla configurazione precedente prima del lunedì, **Verifica pre-apertura**: il team IT può verificare il corretto funzionamento lunedì mattina prima dell'arrivo degli utenti

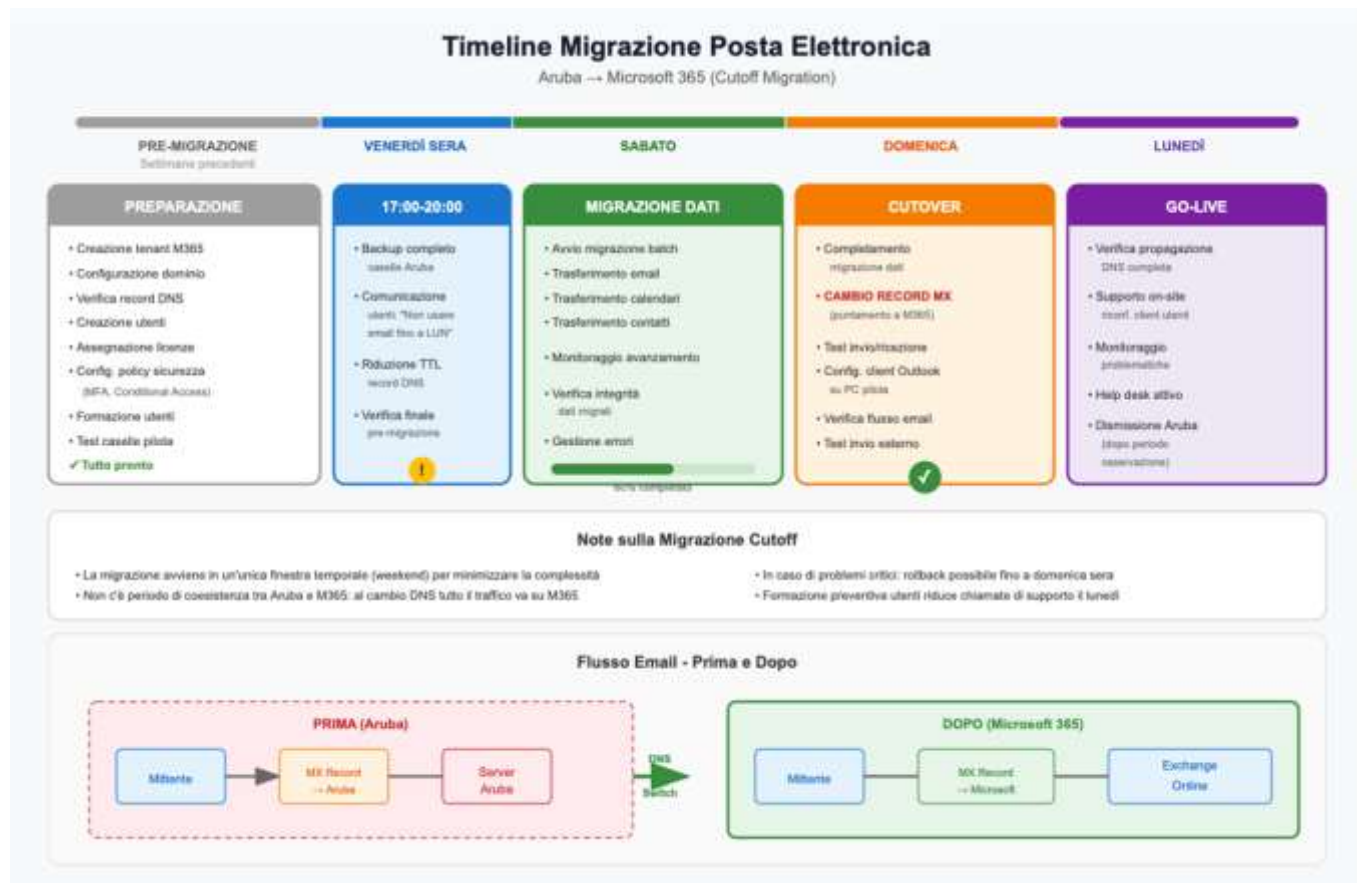
#### TIER 1 srl

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it



## 6.2.2 Fasi della Migrazione



### Timeline Migrazione Posta

Figura: Timeline dettagliata della migrazione email con fasi Pre-migrazione, Venerdì, Sabato, Domenica e Lunedì

## 6.2.3 Razionalizzazione Caselle Email

In occasione della migrazione, verrà effettuata una **razionalizzazione delle caselle email** esistenti. Alcune caselle attualmente separate verranno consolidate in un'unica casella in base alle nuove esigenze organizzative dell'ente.

Questa attività di razionalizzazione permette di: **Semplificare la gestione**: meno caselle da amministrare, **Ridurre i costi**: ottimizzazione del numero di licenze necessarie, **Migliorare l'organizzazione**: struttura email più aderente all'organigramma attuale, **Eliminare ridondanze**: caselle obsolete o non più utilizzate

La mappatura finale delle caselle (situazione target) è riportata nella tabella seguente.



#### 6.2.4 Mailbox Target (Post-Migrazione)

#	Mailbox	Licenza
1	antonella.archetti@comune.monteisola.bs.it	Business Standard
2	biblioteca@comune.monteisola.bs.it	Business Standard
3	claudio.pasinetti@comune.monteisola.bs.it	Business Standard
4	cristiana.agnesi@comune.monteisola.bs.it	Business Standard
5	finanziario@comune.monteisola.bs.it	Business Standard
6	gianluigi.turla@comune.monteisola.bs.it	Business Standard
7	giuliana.archetti@comune.monteisola.bs.it	Business Standard
8	giuseppe.scolaro@comune.monteisola.bs.it	Business Standard
9	lorenzo.zilani@comune.monteisola.bs.it	Business Standard
10	massimiliano.mazzucchelli@comune.monteisola.bs.it	Business Standard
11	paola.turla@comune.monteisola.bs.it	Business Standard
12	protezione.civile@comune.monteisola.bs.it	Business Standard
13	sergio.turla@comune.monteisola.bs.it	Business Standard
14	siglinde.turla@comune.monteisola.bs.it	Business Standard
15	turistico@comune.monteisola.bs.it	Business Standard
16	alberto.bernardi@comune.monteisola.bs.it	Business Standard
17	lidia.sanzogni@comune.monteisola.bs.it	Business Standard



### 6.3 Licenze Microsoft 365

Licenza	Quantità	Funzionalità
Business Standard	17	Exchange, Office Apps, Teams, SharePoint, OneDrive
Defender for Office365 P1	17	Protezione avanzata antispam & mail protect
Entra ID P2	1	Conditional Access, Identity Protection, PIM
Exchange Online P1	2	Caselle shared/service aggiuntive
Microsoft 365 Copilot	2	Assistente AI per produttività

### 6.4 Migrazione Dati

Origine	Destinazione	Contenuto
File server locale	SharePoint Online	Documenti condivisi
Cartelle utente	OneDrive for Business	Documenti personali

#### 6.4.1 Prerequisiti e Limiti di Storage

La licenza Microsoft 365 Business Standard include uno storage SharePoint condiviso di **1 TB base + 10 GB per utente**. Per il Comune di Monte Isola (17 utenti), lo storage totale disponibile è di circa **1,17 TB**.

Voce	Dettaglio
Storage SharePoint incluso	1 TB + 10 GB/utente (~1,17 TB totali)
Storage OneDrive per utente	1 TB per utente
Limite dati da migrare	≤ 1 TB

#### TIER 1 srl

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





#### Prerequisito fondamentale:

La mole di dati da migrare su SharePoint Online **non deve superare 1 Terabyte**. Qualora il volume dei dati presenti sul file server locale ecceda questo limite, sarà necessario valutare l'acquisto di storage aggiuntivo Microsoft 365 o licenze con maggiore capacità, con conseguente incremento dei costi di progetto.

#### Utilizzo di OneDrive for Business:

È importante evidenziare che, oltre allo storage SharePoint condiviso, ogni utente dispone di un archivio personale **OneDrive for Business con capacità di 1 TB ciascuno**. Per i file che non necessitano di condivisione tra diversi uffici o che sono di pertinenza esclusiva di un singolo dipendente, è possibile sfruttare questo spazio di archiviazione individuale. Questa opzione consente di:

- Alleggerire il volume di dati da migrare su SharePoint
- Sfruttare appieno le risorse incluse nella licenza Business Standard
- Mantenere i documenti personali separati da quelli condivisi
- Garantire comunque backup, sincronizzazione e accessibilità da qualsiasi dispositivo

#### 6.4.2 Attività Propedeutiche a Carico del Cliente

A livello di progetto è previsto che il Comune di Monte Isola, prima dell'avvio della migrazione, svolga le seguenti attività preparatorie:

1. **Razionalizzazione dei file:** revisione e pulizia dei documenti presenti sul file server, con eliminazione di:
  - File duplicati
  - Versioni obsolete di documenti
  - File temporanei e non più necessari
  - Contenuti personali non pertinenti all'attività lavorativa
2. **Predisposizione archivio storico:** identificazione e separazione dei file non più in utilizzo corrente, da archiviare su supporto separato (NAS locale, storage offline o archivio cloud a basso costo) e non oggetto di migrazione su SharePoint
3. **Mappatura della struttura:** definizione della nuova struttura di cartelle SharePoint in base alle esigenze organizzative dell'ente

Queste attività sono essenziali per: - Garantire il rispetto dei limiti di storage inclusi nella licenza, Ottimizzare i tempi di migrazione - Migliorare l'organizzazione documentale post-migrazione, Evitare costi aggiuntivi non previsti



## 6.5 Domain Controller

### 6.5.1 Configurazione Attuale

Voce	Valore
Ubicazione	On-premise (Municipio)
Sistema Operativo	Windows Server 2008 R2
Ruolo	Domain Controller Active Directory

### 6.5.2 Configurazione Target

Voce	Valore
Ubicazione	Datacenter Brescia
Sistema Operativo	Windows Server 2022/2025 Standard
Certificazione DC	ISO 27001
Tipo migrazione	Reinstallazione pulita (no upgrade)
Entra ID	Non previsto (vincoli applicativi)

### 6.5.3 Alta disponibilità e ripristino DC

Il Domain Controller sarà ospitato come singola VM nel datacenter ISO 27001, ma su infrastruttura hypervisor ridondata (cluster con HA host e storage). Per mitigare il rischio di SPOF logico sono previsti backup giornalieri del DC con verifica periodica dei restore in ambiente isolato. Il DC potrà essere rialzato su host alternativo in caso di fault hardware; eventuale ripristino da backup seguirà una procedura testata e documentata.

#### **TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it



## 7. BACKUP E DISASTER RECOVERY

Il backup dei dati e la capacità di ripristino in caso di disastro rappresentano l'ultima linea di difesa di qualsiasi organizzazione. Quando tutte le altre misure di sicurezza falliscono, che si tratti di un attacco ransomware riuscito, di un errore umano che cancella dati critici o di un guasto hardware, è il backup a fare la differenza tra un'interruzione temporanea e una perdita irreversibile.

Per una Pubblica Amministrazione, la perdita di dati può avere conseguenze devastanti: documenti anagrafici, atti amministrativi, dati finanziari e comunicazioni ufficiali sono patrimonio dell'ente e dei cittadini che serve. Il GDPR impone inoltre obblighi specifici sulla capacità di ripristinare tempestivamente la disponibilità dei dati personali in caso di incidente.

È fondamentale comprendere che la migrazione verso servizi cloud come Microsoft 365, pur offrendo enormi vantaggi in termini di disponibilità e ridondanza dell'infrastruttura, **non elimina la necessità di una strategia di backup dedicata**. Microsoft opera secondo il modello di "Shared Responsibility" (responsabilità condivisa): il provider garantisce la disponibilità del servizio e la protezione dell'infrastruttura, ma la protezione dei dati del cliente rimane responsabilità del cliente stesso.

Questo capitolo descrive la strategia di backup adottata per proteggere sia i dati in cloud (Microsoft 365) sia i dati locali durante la fase transitoria.

### 7.1 Backup Microsoft 365

Voce	Dettaglio
Prodotto	Acronis Cyber Protect (SaaS)
Retention	365 giorni
Frequenza	Backup giornaliero
Oggetti protetti	Exchange Online, SharePoint, OneDrive
Storage	Cloud in Unione Europea
Crittografia	AES-256 in transit e at rest
Compliance	GDPR certificato

#### 7.1.1 Backup fase transitoria (VM locali)

Durante la fase transitoria le VM legacy on-premise saranno protette con software di backup locale dedicato. Sono previsti backup full + incrementali con retention 30-60 giorni, salvataggio sull'attuale NAS ricondizionato e posto in una VLAN isolata; ove disponibile, sarà attivata l'opzione di immutabilità/offline. È richiesto un test di ripristino trimestrale per validare i backup. RPO target: 24h; RTO target: 8h per le VM critiche transitorie. Acronis rimane la soluzione unica per Microsoft 365 (retention 365 giorni).



## 7.2 Motivazione (Shared Responsibility Model)

Microsoft garantisce la disponibilità dell'infrastruttura ma **non** la protezione dei dati da: Cancellazioni accidentali degli utenti - Cancellazioni malevole (insider threat) - Ransomware che cifra i dati sincronizzati - Requisiti di retention oltre i limiti Microsoft

## 7.3 Backup Server Locale (Fase Transitoria)

Durante la fase transitoria, implementazione/mantenimento di backup locale per: Server applicativi legacy (Sicraweb, Concilia, Re-Rite) - Protezione dati fino a completamento migrazione SaaS - Dismissione solo dopo verifica integrità dati migrati

# 8. FASE TRANSITORIA

Ogni progetto di trasformazione IT deve confrontarsi con la realtà dell'esistente. Non è possibile, né auspicabile, sostituire in un colpo solo tutti i sistemi: alcuni applicativi sono critici per l'operatività quotidiana, altri dipendono da fornitori terzi con tempistiche proprie, altri ancora richiedono verifiche approfondite prima di poter essere dismessi.

La fase transitoria è quel periodo di coesistenza tra vecchio e nuovo in cui particolare attenzione deve essere posta per garantire: -

**Continuità operativa:** i servizi ai cittadini non devono subire interruzioni - **Integrità dei dati:** nessun dato deve andare perso durante le migrazioni - **Sicurezza:** anche i sistemi legacy devono essere protetti adeguatamente fino alla dismissione - **Coordinamento:** le attività devono essere sincronizzate con i fornitori esterni (Maggioli, INTRED)

Nel caso del Comune di Monte Isola, la fase transitoria riguarda principalmente gli applicativi gestionali Maggioli (Sicraweb, Concilia) che sono ancora parzialmente o totalmente installati sul server locale. La migrazione di questi applicativi verso la modalità SaaS (Software as a Service) è di competenza del produttore Maggioli e richiede un coordinamento preciso per evitare discontinuità di servizio.

Durante questa fase, il server locale esistente viene mantenuto operativo e protetto (backup, antivirus, accesso controllato) fino al completamento delle migrazioni SaaS e alla verifica dell'integrità dei dati migrati. Solo dopo questa verifica si procederà alla dismissione definitiva.

## 8.1 Applicativi Legacy

Applicativo	Produttore	Stato Attuale	Target
Sicraweb	Maggioli	Parzialmente SaaS	Migrazione completa SaaS
Concilia	Maggioli	On-premise	Migrazione SaaS
Re-Rite	-	On-premise	Da definire





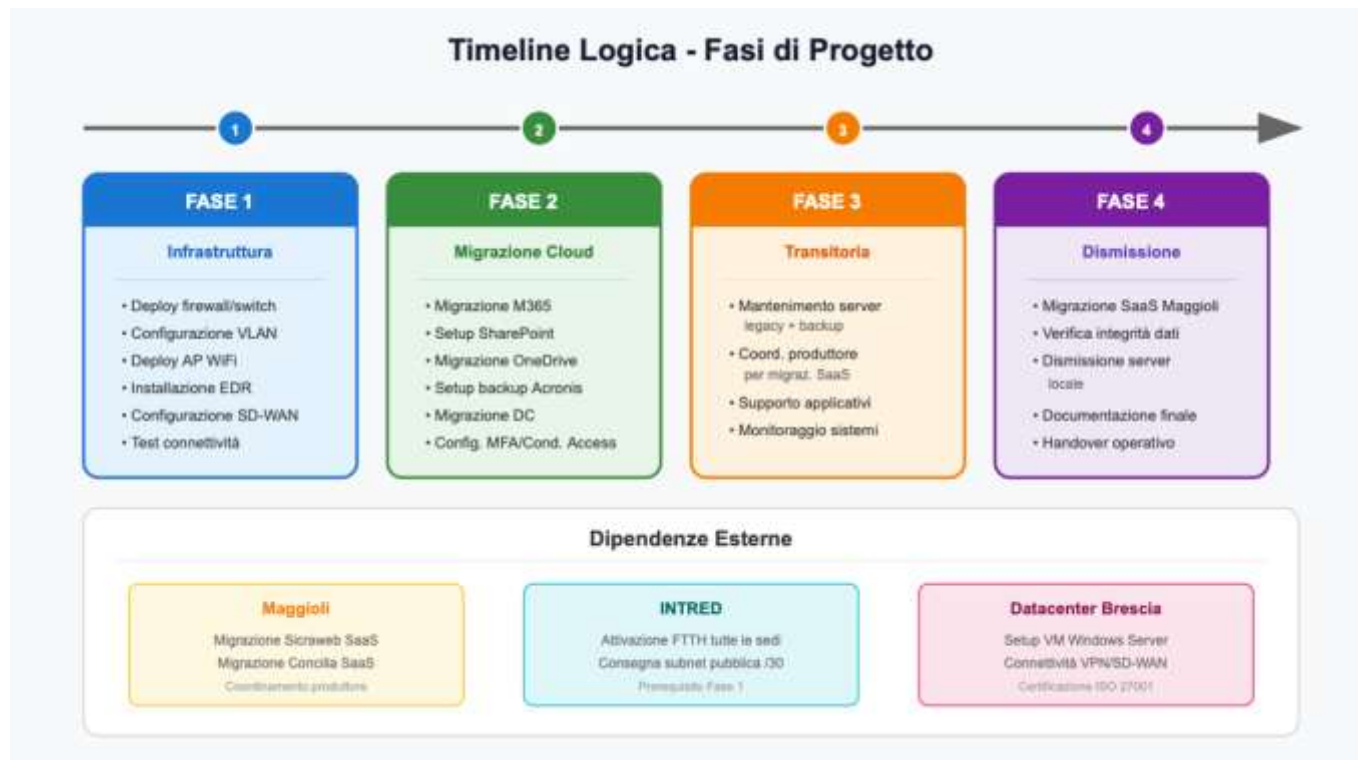
### 8.1.1 Perché la Migrazione SaaS è la Scelta Ottimale

La migrazione degli applicativi gestionali verso la modalità **SaaS (Software as a Service)**, erogata direttamente dal produttore del software, rappresenta la strategia preferibile rispetto a qualsiasi altra soluzione alternativa. In un modello SaaS, il produttore si assume la piena responsabilità dell'infrastruttura, della manutenzione, degli aggiornamenti e della sicurezza dell'applicativo: il cliente accede al servizio tramite browser o client leggero, senza dover gestire server, sistemi operativi, database o componenti middleware. Questo approccio garantisce che l'applicativo sia sempre aggiornato all'ultima versione, con patch di sicurezza applicate tempestivamente dal vendor e funzionalità evolute rilasciate in modo continuo. Per un ente pubblico di piccole dimensioni come il Comune di Monte Isola, che non dispone di personale IT dedicato, delegare al produttore la complessità tecnica della gestione applicativa significa potersi concentrare esclusivamente sull'utilizzo del software per l'erogazione dei servizi ai cittadini.

L'alternativa comunemente proposta, il cosiddetto approccio **"lift and shift"**, che consiste nel trasferire il server esistente (o una sua copia virtualizzata) in un datacenter esterno o in un cloud IaaS (Infrastructure as a Service), è una soluzione che presenta significative inefficienze e rischi residui. In questo scenario, il server viene semplicemente "spostato" da una collocazione fisica a un'altra, ma tutte le responsabilità di gestione rimangono invariate: il cliente deve continuare a occuparsi degli aggiornamenti del sistema operativo, delle patch di sicurezza dell'applicativo, dei backup, del monitoraggio, della gestione dei certificati e della risoluzione di eventuali problemi tecnici. Di fatto, si tratta di un "falso cloud" che non offre i reali benefici della trasformazione digitale. Il server virtualizzato in datacenter invecchia esattamente come invecchiava on-premise, accumulando debito tecnico, vulnerabilità non corrette e incompatibilità con le nuove tecnologie. Inoltre, i costi operativi (hosting, banda, supporto sistemistico) si sommano ai costi di licenza software, rendendo la soluzione economicamente meno vantaggiosa nel medio-lungo periodo.

Dal punto di vista della **sicurezza e della responsabilità**, la differenza tra i due approcci è sostanziale. Con il lift and shift, il cliente mantiene la piena responsabilità della sicurezza del workload: se il server viene compromesso a causa di una vulnerabilità non patchata, la responsabilità è dell'ente. Con il modello SaaS, invece, la sicurezza dell'infrastruttura e dell'applicativo è contrattualmente in capo al produttore, che dispone di team dedicati, strumenti avanzati e processi certificati per garantire la protezione del servizio. In caso di incidente, il produttore SaaS è tenuto a intervenire, ripristinare il servizio e notificare l'accaduto secondo gli SLA contrattuali. Per il Comune di Monte Isola, che ha già subito un grave attacco informatico, l'adozione del modello SaaS per gli applicativi critici rappresenta non solo una scelta di efficienza, ma una misura concreta di riduzione del rischio cyber, eliminando dalla propria responsabilità diretta componenti che storicamente sono stati vettori di compromissione.

## 8.2 Strategia



### Timeline Fase Transitoria

Figura: Timeline logica delle 4 fasi di progetto (Infrastruttura, Migrazione Cloud, Transitoria, Dismissione) con dipendenze esterne

## 8.3 Dipendenze

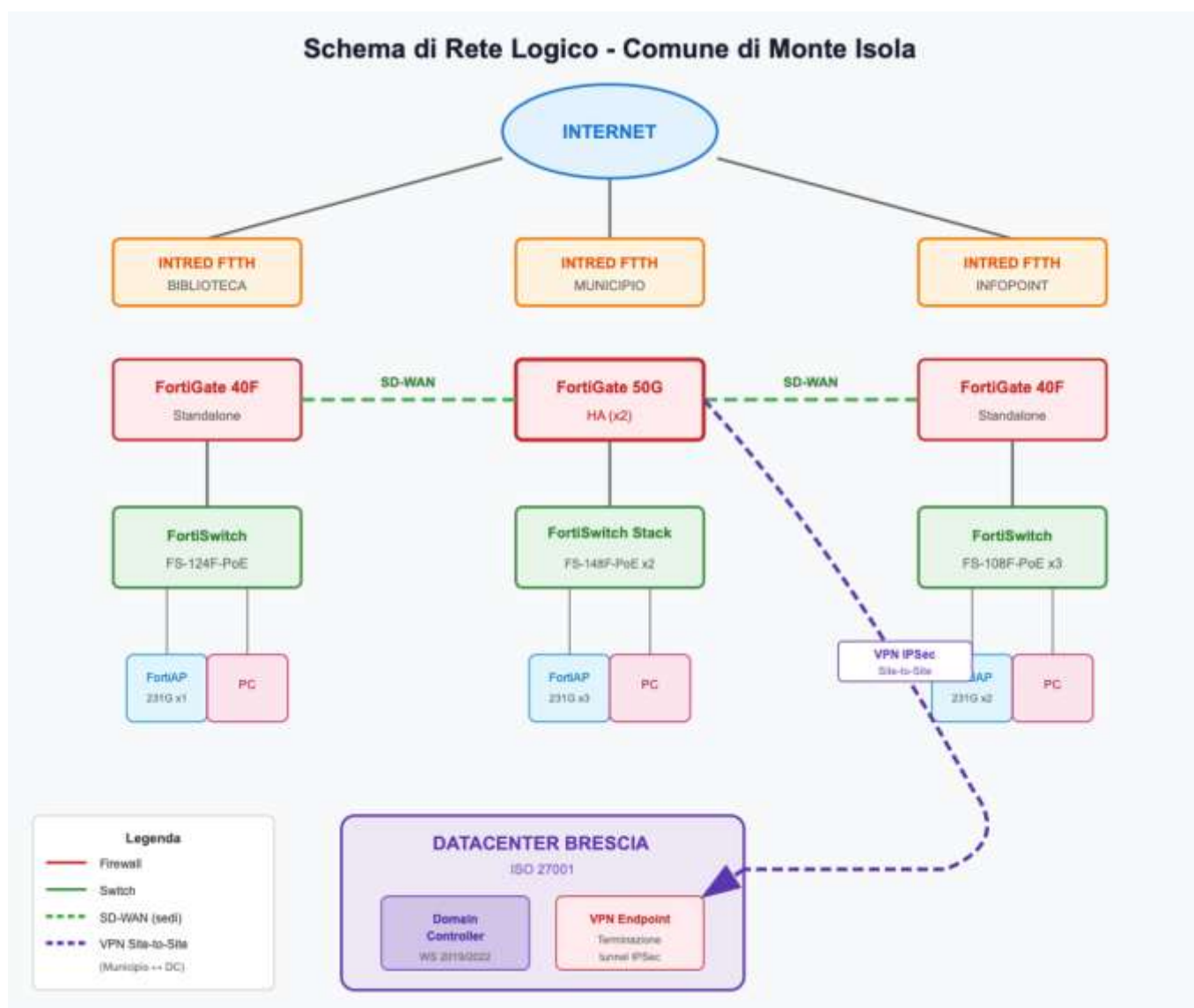
Dipendenza	Owner	Note
Migrazione Sicraweb SaaS	Maggioli	Coordinamento con produttore
Migrazione Concilia SaaS	Maggioli	Coordinamento con produttore
Attivazione FTTH	INTRED	Prevista gennaio 2025

## 9. SCHEMA DI RETE LOGICO

Lo schema di rete logico fornisce una rappresentazione visiva dell'architettura proposta, mostrando come i diversi componenti sono interconnessi tra loro. Questa visualizzazione è fondamentale per comprendere i flussi di traffico, identificare i punti critici e pianificare eventuali interventi futuri.

I diagrammi seguenti illustrano: - La **topologia WAN** con le tre sedi interconnesse via SD-WAN attraverso internet FTTH - La **gerarchia degli apparati** in ogni sede: firewall → switch → endpoint/access point - La connessione al **datacenter esterno** dove risiederà il Domain Controller - Il **dettaglio della segmentazione VLAN** nella sede principale (Municipio)

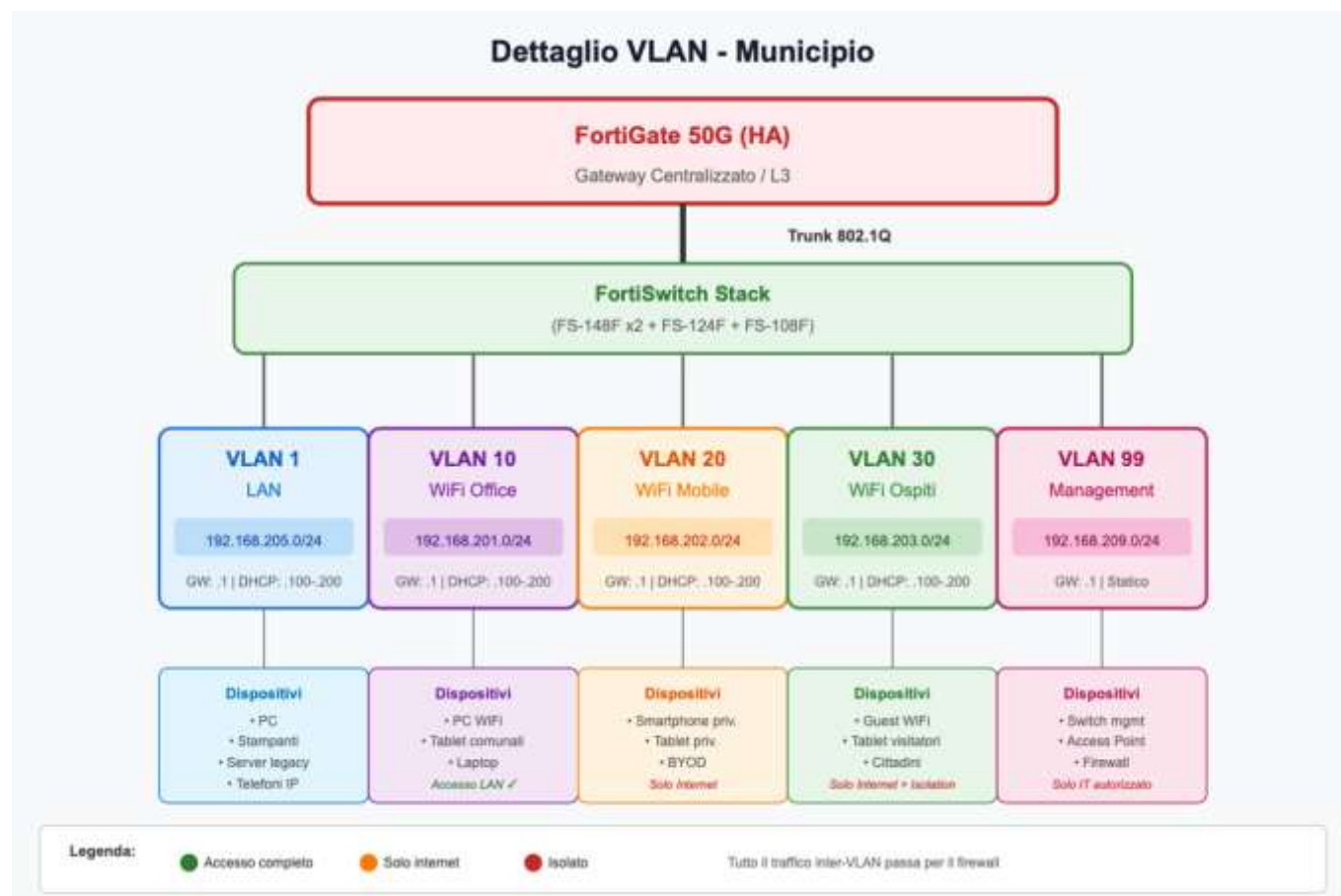
### 9.1 Topologia WAN



Schema di Rete Logico - Topologia WAN

Figura: Schema di rete logico con le 3 sedi (Municipio, Biblioteca, Infopoint) interconnesse via SD-WAN, connessione VPN Site-to-Site al Datacenter di Brescia

## 9.2 Dettaglio VLAN - Municipio



Dettaglio VLAN Municipio

Figura: Dettaglio della segmentazione VLAN nella sede Municipio con indirizzamento IP e dispositivi per segmento

## 10. BILL OF MATERIALS

La Bill of Materials (BOM) rappresenta l'elenco dettagliato di tutti i componenti hardware, software e servizi necessari per la realizzazione del progetto. Questo capitolo fornisce una vista consolidata degli elementi da acquisire, organizzati per categoria.

La BOM è un documento fondamentale per: **Procurement**: base per la richiesta di offerte ai fornitori - **Budgeting**: stima dei costi di progetto - **Inventory**: tracciamento degli asset acquisiti - **Pianificazione**: sequenziamento delle attività di deploy



Le quantità indicate sono state dimensionate sulla base dei requisiti raccolti e includono eventuali ridondanze previste (es. firewall in HA).  
Le licenze software sono indicate con la durata contrattuale raccomandata (3 anni per Fortinet, annuale per Microsoft 365).

#### 10.1 Hardware Network

Categoria	Modello	Quantità	Note
Firewall	FortiGate 50G	2	Municipio - HA
Firewall	FortiGate 40F	2	Biblioteca + Infopoint
Switch	FortiSwitch FS-148F-PoE	2	Municipio
Switch	FortiSwitch FS-124F-PoE	1	Biblioteca
Switch	FortiSwitch FS-108F-PoE	3	Infopoint
Access Point	FortiAP 231G	3	Municipio
Access Point	FortiAP 231G	1	Biblioteca
Access Point	FortiAP 231G	2	Infopoint

#### 10.2 Licenze Fortinet (3 anni)

Apparato	Licenza	Quantità
FortiGate 50G	UTP (Unified Threat Protection)	2
FortiGate 50G	FortiCare Premium	2
FortiGate 50G	FortiCloud	2
FortiGate 40F	UTP (Unified Threat Protection)	2
FortiGate 40F	FortiCare Premium	2

#### TIER 1 srl

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





FortiGate 40F	FortiCloud	2
FS-148F-PoE	FortiCare Premium	2
FS-124F-PoE	FortiCare Premium	1
FS-108F-PoE	FortiCare Premium	3
FortiAP 231G	FortiCare Premium	6

### 10.3 Licenze Microsoft 365 (annuali)

Licenza	Quantità
Microsoft 365 Business Standard	17
Microsoft Defender for Office365 P1	17
Microsoft Entra ID P2	1
Exchange Online Plan 1	2
Microsoft 365 Copilot	2

### 10.4 Endpoint Security

Prodotto	Quantità	Copertura
SentinelOne Complete	~18 agent	15 endpoint + 3 server (stima)

### 10.5 Backup

Prodotto	Quantità	Retention
Acronis Cyber Protect M365	17 mailbox + SharePoint	365 giorni

#### TIER 1 srl

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





#### 10.6 Datacenter

Servizio	Quantità	Specifiche
VM Windows Server	1	Domain Controller
Datacenter	-	Brescia, ISO 27001

#### 10.7 Riepilogo Quantità

Categoria	Totale
Firewall	4
Switch	6
Access Point	6
Licenze Fortinet 3Y	24
Licenze M365	37
Agent EDR	20
Backup M365	17 mailbox

#### TIER 1 srl

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it



## 11. CONFORMITÀ NORMATIVA

La conformità normativa non è un aspetto accessorio del progetto, ma uno dei suoi driver principali. Le Pubbliche Amministrazioni italiane sono soggette a un quadro regolatorio articolato che impone specifici requisiti in materia di sicurezza informatica, protezione dei dati personali e digitalizzazione dei servizi.

Il mancato rispetto di queste normative può comportare: **Sanzioni amministrative**: il GDPR prevede sanzioni fino al 4% del fatturato o 20 milioni di euro - **Responsabilità dirigenziale**: i dirigenti pubblici rispondono personalmente del mancato adeguamento - **Danno reputazionale**: la perdita di fiducia dei cittadini nei servizi digitali dell'ente - **Esclusione da finanziamenti**: l'accesso a fondi PNRR richiede il rispetto delle linee guida AGID

Il progetto è stato progettato fin dall'inizio per garantire piena conformità ai requisiti normativi vigenti, adottando soluzioni certificate e best practice riconosciute. Di seguito il dettaglio delle normative considerate e delle relative implementazioni.

### 11.1 Riferimenti AGID

L'Agenzia per l'Italia Digitale (AGID) definisce le linee guida e i requisiti tecnici che le Pubbliche Amministrazioni devono rispettare in ambito ICT. Il progetto è conforme alle seguenti disposizioni:

Normativa	Applicazione nel progetto
Misure minime di sicurezza ICT per le PA (Circolare AgID 2/2017)	Firewall NGFW, segmentazione VLAN, EDR, MFA, backup
Piano Triennale per l'informatica nella PA	Principio "cloud first" - migrazione M365 e DC in datacenter
Linee guida per la sicurezza nel procurement ICT	Vendor non in blacklist AGID
Qualificazione Cloud Service Provider	Microsoft 365 e Acronis sono CSP qualificati





### 11.2 GDPR

Requisito	Implementazione
Protezione dati personali	Crittografia, backup, access control
Data residency	Storage backup in UE
Diritto all'oblio	Retention policy configurabili
Accountability	Logging e audit trail

### 11.3 Vendor Compliance

Tutti i vendor selezionati rispettano i requisiti AGID: - **Fortinet**: Non in blacklist, ampia adozione PA italiana - **Microsoft**: CSP qualificato, datacenter EU - **Acronis**: GDPR compliant, storage EU - **SentinelOne**: Leader Gartner Magic Quadrant EPP

#### **TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





## 12. GESTIONE POST-PROGETTO

La realizzazione di un'infrastruttura moderna è solo il primo passo: per mantenere nel tempo i benefici ottenuti è essenziale una gestione continuativa professionale. Le tecnologie evolvono, le minacce si aggiornano, le configurazioni richiedono manutenzione e gli utenti necessitano di supporto.

Un ente delle dimensioni del Comune di Monte Isola non dispone delle risorse interne per gestire autonomamente un'infrastruttura di questa complessità. La scelta naturale è affidarsi a un Managed Service Provider (MSP) che possa garantire: **Competenze specialistiche**: personale certificato sulle tecnologie adottate (Fortinet, Microsoft, SentinelOne) - **Monitoraggio continuo**: monitoraggio proattivo 24/7 per identificare problemi prima che impattino gli utenti - **Risposta rapida**: intervento tempestivo in caso di guasti o incidenti di sicurezza - **Aggiornamenti regolari**: patching di sicurezza e upgrade pianificati - **Economia di scala**: costi condivisi con altri clienti del provider

Il fornitore che si aggiudicherà l'appalto per la realizzazione del progetto sarà naturalmente candidato alla gestione post-progetto, avendo già acquisito conoscenza approfondita dell'infrastruttura durante le fasi di deploy e configurazione.

### 12.1 Responsabilità

Voce	Dettaglio
Responsabile	MSP/Fornitore vincitore appalto
Modello	Contratto di manutenzione e supporto
Durata consigliata	Minimo 36 mesi (allineato a licenze Fortinet)

## Appendice A - Glossario

Termine	Definizione
EDR	Endpoint Detection and Response
XDR	Extended Detection and Response
NGFW	Next-Generation Firewall

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it





SD-WAN	Software-Defined Wide Area Network
VLAN	Virtual Local Area Network
HA	High Availability
MFA	Multi-Factor Authentication
NAC	Network Access Control
UTP	Unified Threat Protection
IPS	Intrusion Prevention System
PoE	Power over Ethernet

**TIER 1 srl**

Via Cefalonia, 55  
25124 Brescia (BS) ITALY  
P.IVA e C.F.: 03970990986

hello@tier1.it  
www.tier1.it

