COMUNE DI MALCESINE

PIANO SICUREZZA
REV. 1
OTTOBRE 2019

Studio Piras S.a.s. – via al Desert, 2 – 38122 TRENTO
tel. +390461390902 +3904611933333
mail: info@studiopiras.net web: www.studiopiras.net

COMUNE DI MALCESINE
Piazza Statuto, 1 - Malcesine (VR)
Partita IVA 00601160237

protocollo@pec.comunemalcesine.it

Piano della Sicurezza Informatica

(art. 4, c. 1, lett. C, DPCM 03 dicembre 2013

Art.12, DPCM 13 novembre 2014)

COMUNE DI MALCESINE
Piazza Statuto, 1 - Malcesine (VR)
Partita IVA 00601160237

protocollo@pec.comunemalcesine.it

1 Il piano di sicurezza informatica

1.1 Definizione

Il ricorso alle tecnologie dell'informazione e della comunicazione intrapreso dal Comune per lo snellimento, l'ottimizzazione e una maggiore efficienza dei procedimenti amministrativi, comporta una serie di rischi che, se non adeguatamente affrontati, potrebbero comportare gravi conseguenze sull'affidabilità dei dati e dei servizi. Tali rischi sono imputabili a due fattori caratteristici della tecnologia in questione: la non garanzia di corretto funzionamento sia nelle componenti hardware che in quelle software e l'esposizione alle intrusioni informatiche. In termini più operativi è bene intendere la sicurezza del Sistema Informativo non solo come "protezione del patrimonio informativo da rilevazioni, modifiche o cancellazioni non autorizzate per cause accidentali o intenzionali" ma anche come "limitazione degli effetti causati dall'eventuale occorrenza di tali cause".

Si evidenzia che la sicurezza del Sistema Informativo non dipende solo da aspetti tecnici ma anche, se non principalmente, da quelli organizzativi, sociali e legali. La sicurezza del Sistema Informativo è pertanto vista come caratteristica "globale", in grado di fornire dinamicamente, con l'evolversi temporale delle necessità e delle tecnologie, il desiderato livello di disponibilità, integrità e confidenzialità delle informazioni e dei servizi erogati.

Il presente Piano descrive le misure di sicurezza adottate per la formazione, la gestione, la trasmissione, l'interscambio, l'accesso e la conservazione dei documenti informatici, nel rispetto anche di quanto disposto dal D. Lgs 196/2003, "Codice in materia di protezione dei dati personali" e del relativo Allegato B "Disciplinare tecnico in materia di misure minime di sicurezza". Sono elencate inoltre le strategie ed i controlli adottati per assicurare al Sistema Informativo del Comune un adeguato livello di sicurezza.

1.2 Obiettivi

Scopo del presente documento è descrivere la strategia che il Comune intende adottare per poter soddisfare i seguenti requisiti di sicurezza:

- *Confidenzialità*: l'accesso e la divulgazione delle informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, deve poter essere effettuato solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, la probabilità che un'informazione riservata sia resa pubblica.

- *Integrità*: la modifica o la distruzione di informazioni presenti nel sistema, indipendentemente dal formato in cui si trovano, devono poter essere effettuate solo da entità autorizzate. Devono essere ridotte al minimo, compatibilmente con i limiti delle tecnologie e risorse impiegate, le probabilità che l'informazione sia in qualche modo modificata. Devono essere altresì garantiti sia l'origine del dato (non ripudiabilità) che la sua conformità all'originale (autenticità).

- *Disponibilità*: l'accesso all'informazione e ai sistemi deve essere sempre affidabile e tempestivo. Una perdita di disponibilità si verifica quando a fronte di un'intrusione un sistema diventa non più accessibile da parte degli utenti.

- *Accountability* (Tracciabilità): tutte le azioni che un'entità compie nell'ambito del sistema sono memorizzate in modo tale da poter essere, in tempi successivi, ricondotte in maniera inequivocabile all'entità stessa.

L'adozione di idonee e preventive misure di sicurezza garantisce che il trattamento dei dati personali comuni identificativi, sensibili e/o giudiziari venga effettuato in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, in relazione alle conoscenze acquisite in base al progresso tecnico, alla loro natura e alle specifiche caratteristiche del trattamento.

Il Piano per la sicurezza informatica si basa attualmente sull'analisi dei rischi a cui è esposto il sistema informatico, i relativi dati e documenti in esso contenuti e sulle direttive strategiche stabilite dal vertice del Comune.

Il presente Piano è soggetto a revisione, in funzione dell'estensione del sistema, dell'evoluzione tecnologica, della variazione degli obiettivi dell'organizzazione e del manifestarsi di nuovi o mutati rischi per la sicurezza. In caso di eventi straordinari il Piano è soggetto ad una revisione estemporanea.

1.3 Responsabilità (figure coinvolte)

L'Ente predispone il Piano per la sicurezza informatica ai sensi dell'art.12 del DPCM 13 novembre 2014. Tale piano risulta essere comprensivo del Piano per la sicurezza informatica dei documenti di cui all'art. 4 del DPCM 3 dicembre 2013, relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso, alla conservazione dei documenti informatici, predisposto dal Responsabile della gestione documentale, applicabile nei limiti dirispetto del regolamento.

2 Il sistema informativo Comunale

2.1 Tipologia di servizi offerti

Il Sistema Informativo del Comune di Malcesine è rivolto a soddisfare tutte le esigenze di carattere informativo-informatico, sia dal punto di vista delle esigenze "interne" cioè sostanzialmente provenienti dai servizi interni all'amministrazione stessa sia, quasi sempre indirettamente, provenienti dall'utenza della popolazione residente esterna all'amministrazione.

Nell'uno e nell'altro caso l'esigenza può essere soddisfatta o da un sistema effettivamente interno, fisicamente residente presso sistemi informativi strettamente Comunali, oppure tramite un sistema esterno, reso disponibile da altri enti e al Comune stesso accessibile con le opportune modalità.

2.2 Servizio informativo

2.2.1 Organizzazione

Nel contesto del Sistema Informativo ogni dipendente del Comune di Malcesine deve collaborare, secondo le proprie specifiche funzioni, alla gestione del Sistema Informativo e alla gestione generale della sicurezza.

Tipologia Utenti	Compiti/Responsabilità	Note
Addetti società assistenza hardware e software	Attuazione e messa in opera delle politiche di sicurezza informatica (sistemi antivirus, firewalling, backup, politiche relative alle utenze, …). Verifiche sull'attuazione delle politiche	
Dipendenti Comune (generici)	Rispetto delle norme relative alla Sicurezza Informatica; rispetto delle norme inerenti il trattamento dati	Vedi incarichi specifici a Responsabile o incaricato del trattamento nei settori specifici

2.2.2 Addetti

Nel contesto del Sistema Informativo ogni dipendente del Comune di Malcesine è, in varia misura e con compiti diversi, corresponsabile del Sistema Informativo nel suo complesso. Per quanto concerne la gestione vera e propria della progettazione ed implementazione delle politiche di sicurezza informatica è stata incaricata una società esterna specializzata in tale settore la quale svolge anche attività di assistenza hardware e software.

2.3 Infrastruttura tecnologica

2.3.1 Generalità

L'Infrastruttura Tecnologica del Comune di Malcesine può essere schematizzata come segue:

Tipologia di apparati	Descrizione
Apparati Server interni	Indichiamo in questa categoria tutti gli ambienti server di proprietà comunale o comunque gestiti direttamente, sia fisici che virtuali; tutti gli apparati server interni sono dislocati presso la Sala Server Comunale

Apparati Server Esterni	Indichiamo in questa categoria tutti gli ambienti server, sia fisici che virtuali, gestiti da società esterne o dalla Provincia di Verona, in virtù di contratti stipulati con il Comune
Apparati di Rete	Indichiamo in questa categoria tutti gli apparati (router, switch, hub, …) che concorrono alla connettività fra le sedi Comunali (connettività interna), da e verso Internet (connettività pubblica verso l'esterno)
Apparati Storage, di Backup e Sicurezza	Indichiamo in questa categoria tutti gli

	apparati che concorrono specificatamente alla sicurezza (storage per backup, apparati firewall)
Infrastruttura di Comunicazione	Intendiamo con questo termine l'insieme delle cablature che realizzano, per ogni sede, la connettività LAN, nonché l'infrastruttura di comunicazione fra le sedi (WAN), da e verso Internet
Apparati Client	In questa categoria raggruppiamo tutti gli apparati (PC, Portatili, …) utilizzati dall'utenza interna per l'utilizzo dalle sedi territoriali o in connettività mobile dei servizi Comunali

2.3.2 Struttura fisica

Il sistema informatico dell'Ente è così costituito:

- ✓ ***Server "Microsoft Windows Server 2012"*** con funzioni di *domain controller*, *file server*, *DNS* e *DHCP*; sul quale sono installati i *software "PBX"* , "Civilia" , "Concilia", "Antivirus", "Backup" e "Icewarp" utilizzati dall'Ente
- ✓ ***Server "Linux Centos 8"*** con funzioni di *server*; sul quale sono installati i *software "Folium"* , "Civilia" utilizzati dall'Ente
- ✓ ***NAS*** di rete utilizzati come unità di *storage* per tutti i dati gestiti. I dispositive sono due, uno press il ced del Comune e l'altro presso la Biblioteca
- ✓ ***Server "Sito Internet"*** utilizzato per la visibilità esterna.

La quasi totalità degli elaboratori del domino hanno installato come sistema operativo *"Windows 10"* mentre per alcuni il sistema operativo installato è ancora *"Windows 7"*. È in fase avanzata l'aggiornamento del sistema operativo degli elaboratori con *"Windows 7"* a *"Windows 10"*

Caratteristiche sedi comunali

Sede	Comune	Biblioteca	Polizia Locale	Castello
Collegamento tra sedi	Ponte radio con Biblioteca	Ponte radio con Comune	Lan indipendente per sorveglianza, Lan Comune	Ponte radio con Comune
Video sorveglianza	no	no	no	no
Allarme	si	si	si	nn
Anticendio	Estintori	Estintori	Estintori	Estintori
VPN	no	no	no	no

Caratteristiche uffici

Ufficio				
Denominazione	Ufficio Polizia	Uffici Comunali	Uffici Biblioteca	Uffici Castello
Sede	Polizia Locale	Comune	Biblioteca	Castello
Estintori	/	/	/	/
Accesso	Ingresso sede Comune – Porta chiusa a chiave	Porta chiusa a chiave	Porta chiusa a chiave	Porta chiusa a chiave
Armadi chiusi a chiave	/	/	/	
Allarme	vedi sede	vedi sede	vedi sede	vedi sede
Cassaforte	no	no	no	no
Video sorveglianza	no	no	no	no

Caratteristiche armadio di rete

Armadio di rete				
Denominazione	Armadio Rete Polizia	Armadio Rete 1 Comune Ced	Armadio Rete 2 Comune 1° Piano	Armadio Rete Biblioteca
Ubicazione	Ufficio Apparati Polizia	Ufficio Apparati Sede Comune	Ufficio Apparati Sede Comune	Ufficio Apparati Biblioteca
Dimensioni	/	1800/800/1000 19"	1800/800/600 19"	/
Accesso	Chiuso a chiave	Chiuso a chiave	Chiuso a chiave	Chiuso a chiave
Collegamento tra armadi	Cat5 con armadio Comune	Cat5 con armadio Polizia		
UPS	Generale del Comune	Generale del Comune	Generale del Comune	UPS
Raffreddamento	nn	Ventole	Ventole	nn
Ignifugo	nn	nn	nn	nn
Posizione (terra, appeso, ecc)	Terra	Terra	Muro	

Caratteristiche connettività

Connettività				
Denominazione	Adsl Sede Comune	Adsl Backup comune	Adsl Polizia	Adsl Biblioteca
Tipologia	Wireless	Adsl	Adsl	Adsl
DL	12 m	20 m	20 m	7 m
UL	4 m	1m	1m	512 k
Minimo garantito	4/1	8/256k	Nn	nn
Gestore	Eolo	Eolo	Telecom	Telecom
Ip statico	8	8	1	nn
Voip	nn	nn	nn	nn
Note	nn	nn	nn	Usata pubblico

Caratteristiche apparati di rete

Apparati di rete					
Denominazione	Router 1	Switch 1	Switch 2	Switch 3	Switch 4
Tipologia apparato	Firewall UTM	Switch	Switch	Switch	Switch
Marca e modello	Watchguard M370	HP Procurve 2510g-48	HP Procurve 2510g-48	HP Procurve 4104gl	Netgear Fs728tp
Numero porte	8 configurabili	48	48	48	28
Velocità porte	10/100/1000	10/100/1000	10/100/1000	10/100	10/100 POE
Ubicazione	Armadio Rete Ced	Armadio Rete Ced	Armadio Rete Piano	Armadio Rete Polizia	Armadio Rete Ced
VPN	Si	Nn	nn	nn	Nn
Vlan	Si	Si	Si	Si	Si
DMZ	No	Nn	nn	nn	nn
Moduli attivi	Av7Spam/CF/IPS Apt	Nn	nn	nn	nn
Regole e porte configurate	Si	Nn	nn	nn	Nn
UPS	Si	Nn	nn	nn	Nn
Gestione esterna	Si	Si	Si	Si	Si
Bilanciamento	nn	nn	nn	Nn	nn
Failover	No	nn	nn	nn	nn

Apparati di rete					
Denominazione	Switch 5	Switch 6	Router 2		
Tipologia apparato	Switch	Switch	Router		
Marca e modello	Netgear Fs728tp	ZyXEL gs1900	Microtik		
Numero porte	28	48	1Wan + 1 lan		
Velocità porte	10/100 POE	10/100/1000	10/100		
Ubicazione	Armadio Rete Piano	Armadio Rete Biblioteca	Armadio Rete Ced		
VPN	Nn	Nn	nn		
Vlan	Si	Si	nn		
DMZ	nn	Nn	nn		
Moduli attivi	nn	Nn	nn		
Regole e porte configurate	Nn	Nn	nn		
UPS	Nn	Nn	nn		
Gestione esterna	Si	Si	Si		
Bilanciamento	nn	nn	nn		
Failover	nn	nn	nn		

Caratteristiche gruppo di continuità

Gruppo di continuità			
Denominazione	UPS 1	UPS 2	UPS 3
Ubicazione	Armadio Ced	Armadio Rete Ced	Armadio Rete Ced
Apparati collegati	/	/	/
Potenza	3500	3500	3500
Periodicità test e controllo	nn	nn	nn
Gruppo elettrogeno	nn	nn	nn
Montaggio	Base armadio	Base armadio	Base armadio

Caratteristiche storage

Storage		
Denominazione	Nas Ced	Nas Biblioteca
Tipologia	NAS	NAS
Marca e modello	Qnap	Qnap
Numero dischi	4	4
Raid	5	5
Capacità totale/libero	12 TB / variabile > 1 gb	12 TB / variabile > 1 gb
Tipologia dischi	4*4TB GB Sata	4*4TB GB Sata
Ubicazione	Ced	Armadio Biblioteca
Montaggio	Scrivania	Scrivania
Numero porte di rete	2	2
Velocità porte	10/100/1000	10/100/1000
Modalità aggiornamento	Manuale	Manuale
Periodicità aggiornamento	Semestrale	Semestrale
UPS	Rack Ced	Rack Biblioteca
Gestione esterna	Si	Si

Caratteristiche server

Server		
Denominazione	Server 1	Server 2
Tipologia	Server Virtuale	Server Virtuale
Marca e modello	Dell	Dell
Ubicazione	Ced	Ced
Processori	Intel Xeon E5-2430 2.20GHz	Intel Xeon E5-2430 2.20GHz
Sistema operativo	Windows 2016 x64	Debian Linux
Funzioni	DC, DHCP, DNS, Pbx, AV	Oracle
UPS	si	si

Server		
Denominazione	Server 4	Server 6
Tipologia	Server Virtuale	Server Virtuale
Marca e modello	Dell	Dell
Ubicazione	Ced	Ced
Processori	Intel Xeon E5-2430 2.20GHz	Intel Xeon E5-2430 2.20GHz
Sistema operativo	Windows 2012 x64	Windows 2012 x64
Funzioni	Concilia	Rdp
UPS	si	Si

Server		
Denominazione	Server 7	FIleserver
Tipologia	Server Virtuale	Server Virtuale
Marca e modello	Dell	Dell
Ubicazione	Ced	Ced
Processori	Intel Xeon E5-2430 2.20GHz	Intel Xeon E5-2430 2.20GHz
Sistema operativo	Debian Linux	Windows 2012 x64
Funzioni	Folium	Dati, Posta, Civilia Open
UPS	si	si

Server		
Denominazione	VC	
Tipologia	Server Virtuale	
Marca e modello	Dell	
Ubicazione	Ced	
Processori	Intel Xeon E5-2430 2.20GHz	
Sistema operativo	Windows 2008 r2	
Funzioni	Servizi, Backup	
UPS	si	

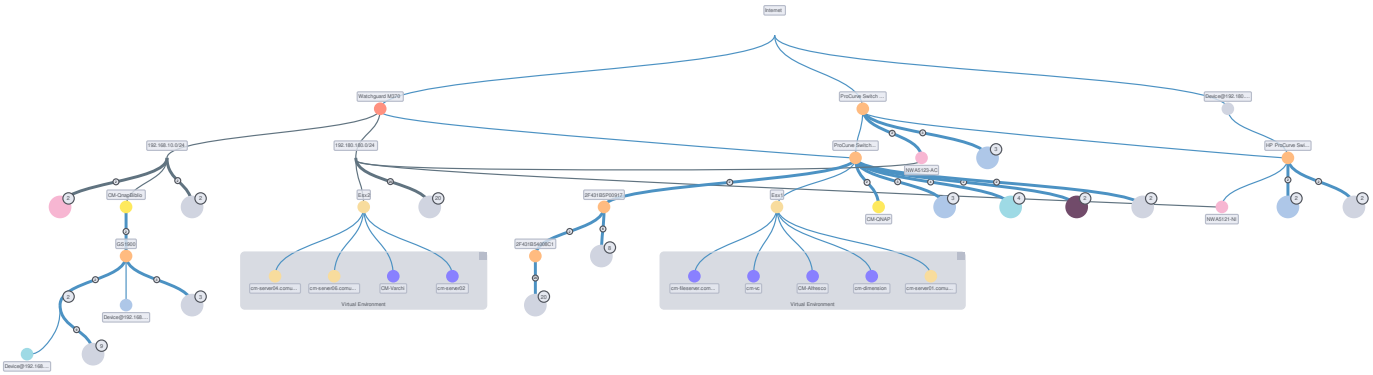
Caratteristiche linee

Linee Analogiche			
Denominazione	Borchia 1	Borchia 2	Borchia 3
Tipo linee	Isdn	Isdn	Isdn
Ubicazione	CED	CED	CED
Gestore	Telecom	Telecom	Telecom

Caratteristiche centralino

Tipologia	Centralino VOIP
Marca e modello	3cx
Linee	16 conversazioni
Ubicazione	CED
Montaggio	VM
UPS	si

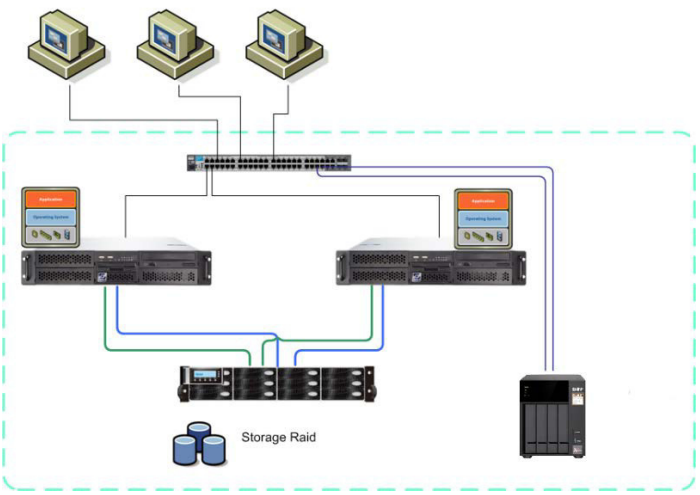
Descrizione grafica dell'infrastruttura comunale



L'infrastruttura fisica è realizzata con 2 host e 1 SAN.

Ogni parte del Sistema è ridondata: 2 alimentatori per gli host così come per la SAN; 2 schede di interfaccia sia negli host che nella SAN.

I dischi ospitati nella SAN sono organizzati con tolleranza RAID5 e RAID 6



L'hypervisor in uso è Vmware, regolarmente licenziato e aggiornato.
Giornalmente viene effettuato un backup sull'unita NAS presso il CED, attraverso un software dedicato (Veeam) che è in grado di gestire uno storico di 14 giorni.
Mensilmente una copia viene effettuata su un altro NAS posizionato in biblioteca, in grado di gestire uno storico annuale. Il backup remoto è in fase di progetto.

Sono presenti due connettività gestite tramite firewall Watchguard.
Una è la principale e l'altra il backup, che si attiva dopo 1 minuto di assenza della primaria.

Il firewall gestisce a bordo una serie di servizi:

- Gateway antivirus
- Gateway spam
- Content filter
- IPS
- Apt blocker

I servizi di posta sono gestiti internamente attraverso un server dedicato (Icewarp)
E' presente una sede per la polizia locale dotata di una proprio connettività.
I pc della polizia locale sono direttamente connessi alla lan comunale.
Sono configurati sul firewall del comune delle regole di accesso/uscita per tutti gli apparati gestiti dalla polizia: videosorveglianza, parchimetri, ecc.
La biblioteca è collegata alla lan comunale attraverso un ponte radio su cui è attestata una VPN.
E' presente poi un ufficio dislocato per servizi presso il Castello caratterizzato da una sola postazione con una propria connettività senza nessun accesso alla rete comunale.

2.3.2.1 PEC

Per quanto concerne la PEC si rimanda alle indicazioni contenute nel Manuale di Gestione

2.3.3 Architettura applicativa

Nel presente paragrafo descriviamo i principali software applicativi ed utilità in uso presso il Comune di Malcesine esplicitandone le caratteristiche salienti.
Dal punto di vista della architettura applicativa possiamo distinguere le seguenti categorie:

a) Software centralizzati: trattasi di applicativi in uso a livello Comunale installati in unica posizione, su server presso la sala server Comunale, in uno degli ambienti virtuali di cui al precedente paragrafo, oppure resi disponibili da enti esterni e usufruibili dal Comune via Web. Quasi sempre la architettura elaborativa è a 3 livelli, composta da un database server, da un application (e web) server con accesso dei client via Web tramite la Intranet Comunale.
b) Software stand-alone: in questa categoria intendiamo software installati localmente sulle postazioni di lavoro, essenzialmente ai fini della produttività personale.

2.3.4 Sistema di Conservazione

Per quanto concerne il sistema di conservazione si fa rimando a quanto dettagliato nel Manuale di Gestione.

3 Politiche organizzative della sicurezza

3.1 Generalità

La definizione e l'applicazione delle politiche di sicurezza all'interno del Comune richiedono l'individuazione di un insieme di regole che fanno riferimento alle tecnologie usate, alle metodologie, alle procedure d'implementazione e ad altri elementi specifici dell'ambiente e del sistema informativo. L'applicazione delle politiche di sicurezza all'interno del Comune richiede, inoltre, la definizione di processi che descrivano gli specifici passi operativi che le persone devono seguire per raggiungere gli obiettivi che sono stati stabiliti. I processi sono indispensabili per la gestione di tutti gli oggetti legati alla sicurezza.

Attualmente, l'individuazione della politica di sicurezza Comunale determina il modello logico della sicurezza fissandone gli obiettivi. L'individuazione degli obiettivi di sicurezza si traduce in obiettivi del sistema informativo, sostanziandosi con la formalizzazione di norme organizzative e standard di riferimento. Inoltre, la sicurezza viene considerata da tutto il personale, una componente integrante dell'attività quotidiana, finalizzata alla protezione delle informazioni e delle apparecchiature da manomissioni, uso improprio o distruzione. Un sistema di sicurezza, per poter raggiungere i migliori risultati funzionali, va visto globalmente, negli aspetti fisici, logici e organizzativi, come un insieme di misure e strumenti hardware, software, organizzativi e procedurali integrati fra loro, volti a ridurre la probabilità di danni a un livello accettabilmente basso e ad un costo ragionevole.

3.1.1 Backup

I dati, in qualunque modo elaborati dal sistema informatico dell'Ente, sono salvati nella memoria centrale dei *Server*. È stato attivato un sistema di duplicazione e memorizzazione dei dati informatici presenti sulle strutture *hardware* del Comune di Malcesine in modalità locale.

3.2 Sicurezza logica

3.2.1 Introduzione

La sicurezza logica si occupa della protezione dell'informazione, dei dati, dei documenti, delle applicazioni, dei sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo. La realizzazione della sicurezza logica è pensata in termini architetturali e ciò comporta l'individuazione di tutti i sistemi hardware e software che implementano le attività dei vari servizi Comunali, in modo tale da garantirne la fruibilità nel tempo, che deve essere nel contempo aperta a tutti gli operatori necessari, ma limitata alle funzioni ad essi attribuite in un determinato momento.

3.2.2 Sistema di autenticazione

La credenziale di autenticazione consiste in un codice per l'identificazione dell'Incaricato (utente), associato a una parola chiave riservata e conosciuta solamente dal medesimo. La parola chiave è composta da almeno otto caratteri (numeri e lettere) e non contiene riferimenti agevolmente riconducibili all'Incaricato, il quale provvederà a modificarla al primo utilizzo. Le credenziali di autenticazione sono affidate al controllo del *Server "Windows 2012"* che garantisce l'applicazione delle politiche di protezione e sicurezza in forma centralizzata ed automatizzata. La politica di centralizzazione del sistema informativo si appoggia al sistema integrato di *active directory* ("insieme di servizi di rete - *account* utente, *account computer*, cartelle condivise, stampanti, *etc*. - adottati dai sistemi operativi organizzati in modo da consentirne la condivisione da parte dei *client*") tramite apposita profilazione degli utenti (gestione dei profili di autorizzazione). Ad integrare la protezione sul sistema informativo, i *software* dell'Ente e gli applicativi *web* sono dotati di apposite procedure di accesso tramite *username* ("nome con il quale l'utente viene riconosciuto da un *computer*, da un programma o da un *server*") e *password* ("sequenza di caratteri alfanumerici utilizzata per accedere in modo esclusivo ad una risorsa informatica"). Lo *username* è un identificativo che, insieme alla *password*, rappresenta le credenziali per accedere alle risorse informatiche o ad un sistema.

3.2.3 Antivirus e similari

Il sistema informatico dell'Ente e i dati personali da esso custoditi sono protetti contro il rischio di intrusione e contro l'azione di programmi di cui all'Articolo 615-*quinquies* del Codice Penale ("*Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico*"), mediante l'attivazione:

- *software antivirus "Symantec Endpoint Protection"* per il *Server "Microsoft"* e i singoli elaboratori,
- *software antivirus* "*Kaspersky"* per la posta elettronica mediante l'*antivirus* integrato nel *Server* di posta elettronica,
- *software antivirus* "*Kaspersky"* per la navigazione attraverso l'antivirus presente nel firewall.
- *software antispam* integrato nel *Server* di posta elettronica, Spam Assasin
- *software antispam* integrato nel *Server* di posta elettronica, Spam Assasin

I sistemi operativi degli elaboratori e del *Server "Microsoft"* sono periodicamente aggiornati automaticamente mediante *Windows Update* con le opportune *patch* di sicurezza ("programma o parte di programma che aggiorna e corregge un *software*").

Un sistema di patch semiautomatico è installato su uno dei server "*"Microsoft"* (Manage Engine Desktop Central) che permette una gestione più accurata del patch management.

Gli aggiornamenti dei programmi per elaboratore volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne difetti sono stati correttamente installati. I programmi sono stati impostati in modo da scaricare e aggiornare automaticamente le loro funzionalità garantendone quindi sempre la massima efficacia di funzionamento.

Al fine di prevenire intrusioni dall'esterno sono stati installati e configurati due *firewall hardware "Watchguard M370"* presso il comune e *"Watchguard XTM330"* presso la biblioteca, entrambi completi delle componeti UTM attive.
Di recente si è preferito utilizzare un solo firewall centrale (*"Watchguard M370"*) in modo da ridurre i costi di gestione e delle licenze software.

Periodicamente sono stati eseguiti e verranno effettuati, nei tempi previsti dalla normativa, gli aggiornamenti sui sistemi di protezione.

4 Documenti e Banche dati

4.1 Sistema di gestione informatica dei documenti

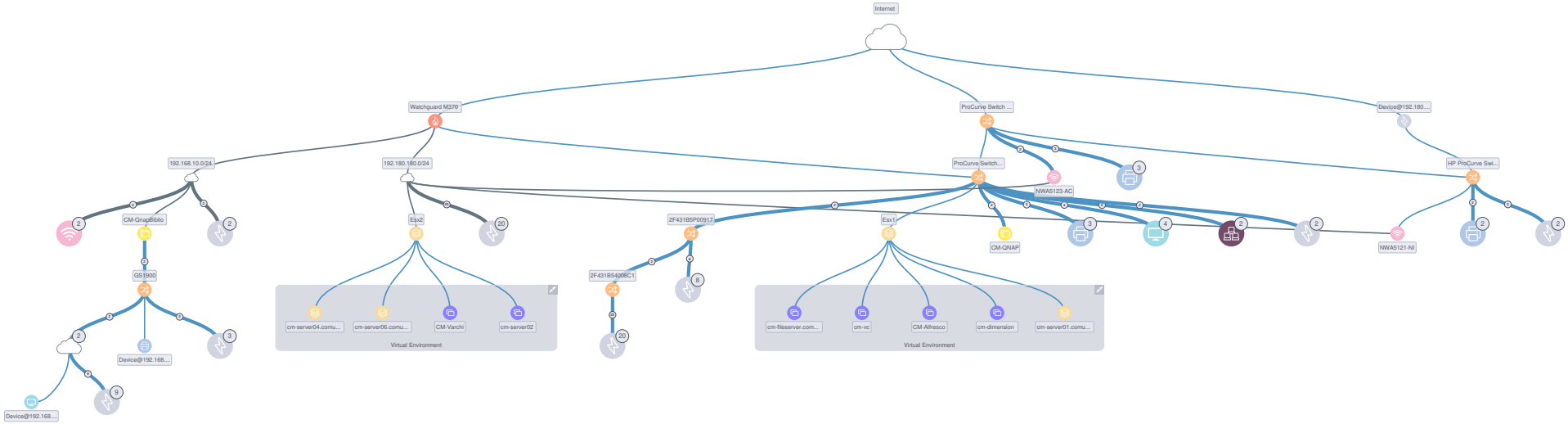
Il DPR 445/2000, all'art. 1, comma 1, lett. r) definisce il Sistema di Gestione Informatica dei Documenti come *"l'insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle amministrazioni per la gestione dei documenti"*. Tale sistema è attivato dal Comune su tutte le postazioni di lavoro degli uffici afferenti all'AOO e le abilitazioni all'utilizzo delle sue funzionalità sono stabilite e aggiornate a cura dei Responsabili individuati all'interno dell'AOO (Responsabile della gestione documentale, Responsabile dei sistemi informativi). Per quanto concerne i software attraverso i quali viene registrato e gestito il patrimonio documentale dell'ente si fa riferimento alle indicazioni contenute nel manuale di gestione così come anche per i seguenti argomenti:

- Protocollo informatico;
- Formazione dei documenti;
- Formati adottati;
- Sottoscrizioni;
- Validazione temporale;
- Metadati;
- Trasmissione dei documenti;
- Conservazione.

5 Trattamento dei dati personali - Analisi dei rischi

Per quanto concerne le politiche inerenti il trattamento dei dati personali e l'analisi dei rischi incombenti sui dati ed i documenti si fa esplicito rimando al ruolo di D.P.O e alle politiche di sicurezza adottato dal Comune di Malcesine.

COMUNE DI MALCESINE TOPOLOGY



PIRAS STUDIO

COMUNE DI MALCESINE

MISURE MINIME
REV. 3
DICEMBRE 2019

Studio Piras S.a.s. – via al Desert, 2 – 38122 TRENTO
tel. +390461390902 +3904611933333
mail: info@studiopiras.net web: www.studiopiras.net

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	**1**	**1**	**M**	**Implementare un inventario delle risorse attive correlato a quello ABSC 1.4**	L'inventario è implementato attraverso ABSC_ID_1.1.2
1	**1**	**2**	**S**	**Implementare ABSC 1.1.1 attraverso uno strumento automatico**	L'inventario è gestito attraverso il software SpiceWorks, costantemente aggiornato. È utilizzata la versione gratuita.
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Attivato per IP4 e IP6 sul server DHCP
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Viene utilizzato e controllato
1	**3**	**1**	**M**	**Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.**	L'elenco di cui alla misura 1.1.1 è aggiornato. L'aggiornamento dell'elenco è a carico degli Amministratori di Sistema. L'implementazione della misura ABSC_ID_1.1.2 prevede la scansione giornaliera delle risorse IP attraverso il software SpiceWorks
1	3	2	S	**Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.**	L'implementazione della misura ABSC_ID_1.1.2 prevede la scansione giornaliera delle risorse IP attraverso il software SpiceWorks
1	**4**	**1**	**M**	**Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.**	Vedi punto 1.1.1. Vengono utilizzati due strumenti software - SpiceWorks – versione free - Manage Engine Desktop Central – versione 50 utenti – contratto con gestore Sistema Informativo

1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	**1**	**1**	**M**	**Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.**	L'aggiornamento dell'elenco dei software è a carico degli Amministratori di Sistema. Viene utilizzato uno strumento software: - Manage Engine Desktop Central – versione 50 utenti – contratto con gestore Sistema Informativo Sono state date direttive al personale ed agli amministratori di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata agli Amministratori di Sistema, che ne verificano la reale esigenza ed eventualmente provvedono affinché sia installato, come pure che venga aggiornato l'elenco.

					Le abilitazioni all'installazione del software sono stati concessi solamente agli amministratori di sistema (vedi 5.1.1)
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	**3**	**1**	**M**	**Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.**	Viene utilizzato uno strumento software: - Manage Engine Desktop Central – versione 50 utenti – contratto con gestore Sistema Informativo Gli Amministratori di Sistema eseguono periodicamente la verifica del software installato su ciascun dispositivo e comparano il risultato con l'elenco di cui al punto 2.1.1. Eventuale software installato che non risulti nell'elenco viene segnalato ai Responsabili della Transizione Digitale, indicherà le misure da intraprendere Le scansioni sono almeno settimanali.
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	Viene utilizzato uno strumento software: - Manage Engine Desktop Central – versione 50 utenti – contratto con gestore Sistema Informativo

2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	Viene utilizzato uno strumento software: - Manage Engine Desktop Central – versione 50 utenti – contratto con gestore Sistema Informativo
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	**1**	**1**	**M**	**Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.**	Gli Amministratori di Sistema hanno definito e documentato le configurazioni sicure standard per ciascun sistema operativo utilizzato. Per l'inserimento di un nuovo computer all'interno del sistema si seguono i seguenti criteri: - Aggiornamento del sistema - Aggiornamento dei dispositivi di sicurezza integrati nel S.O - Installazione antivirus dell'ente - Inserimento in dominio - Configurazione utenze amministrative locali - Installazione delle applicazioni e periferiche
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	

3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	
3	**2**	**1**	**M**	**Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.**	Vedi ABSC_ID_3.1.1.
3	**2**	**2**	**M**	**Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.**	Sono state date disposizioni agli amministratori di sistema in tale senso. In caso di compromissione viene attivata la procedura descritta in ABSC_ID_3.1.1
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	**3**	**1**	**M**	**Le immagini d'installazione devono essere memorizzate offline.**	Non sono utilizzate immagini di installazione.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Non sono utilizzate immagini di installazione.
3	**4**	**1**	**M**	**Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).**	Per attività di gestione effettuate da reti esterne alla rete comunale vengono utilizzate connessioni VPN o comunque criptate.
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della	

				configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	**1**	**1**	**M**	**Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.**	Viene utilizzato uno strumento software: - Manage Engine Desktop Central – versione 50 utenti – contratto con gestore Sistema Informativo
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Viene utilizzato uno strumento software: - Manage Engine Desktop Central – versione 50 utenti – contratto con gestore Sistema Informativo La scansione è almeno settimanale
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	

4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
4	3	1	S	Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	
4	**4**	**1**	**M**	**Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.**	Viene utilizzato uno strumento software: - Manage Engine Desktop Central – versione 50 utenti – contratto con gestore Sistema Informativo L'aggiornamento del database delle vulnerabilità è almeno settimanale. Durante gli interventi viene aggiornato manualmente.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	**5**	**1**	**M**	**Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.**	*Adottare questa misura mira a ridurre il rischio legato alle vulnerabilità, ma occorre evidenziare che l'applicazione automatica delle patch, periodicamente causerà blocchi delle postazioni di lavoro di tutto l'ente, o dei server, o di software (ad es. Anagrafe)!!!* *Evidentemente AGID ha ritenuto che proteggere l'ente dal rischio del danno da vulnerabilità ha un valore superiore al rischio di danno da fermo dei sistemi.* *Si consiglia di schedulare l'applicazione delle patch in momenti nei quali sia garantita la supervisione e la possibilità di intervento da parte degli Amministratori di Sistema e quando l'impatto di un eventuale fermo sia minimo.*

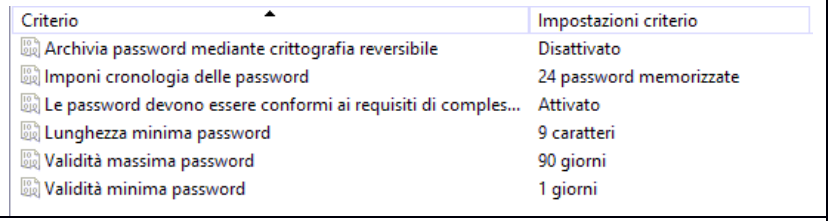
					Viene utilizzato uno strumento software: - Manage Engine Desktop Central – versione 50 utenti – contratto con gestore Sistema Informativo Al momento, vista la recente introduzione dello strumento, le patch sono installate in maniera assistita. Sono automatizzati i processi di aggiornamento dei sistemi operativi Microsoft.
4	**5**	**2**	**M**	**Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.**	Non sono gestiti smartphone e tablet, l'ente non ne è in possesso. Non sono gestiti sistemi non collegati alla rete.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	
4	**7**	**1**	**M**	**Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.**	Sono state date disposizioni agli Amministratori di Sistema di verificare la risoluzione delle vulnerabilità. Nel caso non siano state trovate o applicate le patch necessarie, gli Amministratori di Sistema documentano il caso, le eventuali contromisure o la motivazione della mancato risoluzioni su apposito registro/rapportino conservato presso l'ente. Viene utilizzato uno strumento software: - Manage Engine Desktop Central – versione 50 utenti – contratto con gestore Sistema Informativo
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	
4	**8**	**1**	**M**	**Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).**	E' stato redatto il DPP (*Documento Programmatico in materia di Privacy)* per la gestione del rischio informatico in generale. Occorre redarre il piano richiesto.

					Il piano specifico sarà redatto nel corso dell'anno, periodo legato alle attività necessarie alla fusione con altro ente, con il supporto del Consorzio dei Comuni.
4	**8**	**2**	**M**	**Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.**	Vedi ABSC_ID_4.8.1 Non essendo definito un piano specifico ci attiene alle disposizioni del DPP.
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

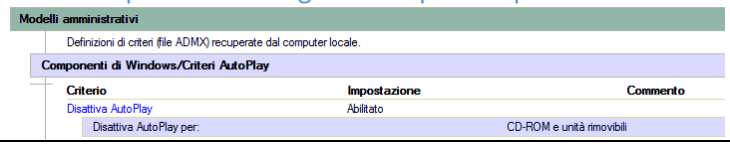
ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	**1**	**1**	**M**	**Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.**	I privilegi di amministratore sono riservati agli amministratori di sistema espressamente nominati da parte dell'ente. I privilegi di amministrazione per smartphone e tablet sono assegnati al soggetto al quale l'apparato è dato in dotazione dato che devono avere la possibilità di accettare in autonomia gli aggiornamenti di sicurezza.
5	**1**	**2**	**M**	**Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.**	E' attivato il log di sistema per registrare gli accessi come amministratore su PC, server, apparati di rete. Viene utilizzato uno strumento software: Business Log – versione 1-79 host
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	

5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	**2**	**1**	**M**	**Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.**	I documenti di nomina degli amministratori di sistema sono consegnati agli stessi e una copia del provvedimento è conservata nell'archivio corrente dell'Ufficio del RTG. L'inventario è gestito da un programma disponibile sul server (KeePass) protetto da password custodita in archivio P3. Viene gestito backup su dispositivo USB custodito in cassetto chiuso a chiave.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	**3**	**1**	**M**	**Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	**7**	**1**	**M**	**Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).**	Account amministrativi: hanno password inserita manualmente, minimo 14 caratteri, senza scadenza. Account user:

					Non devono contenere il nome account dell'utente. Devono essere composte da almeno 9 caratteri. Devono contenere caratteri di almeno tre delle quattro categorie seguenti: Lettere maiuscole dell'alfabeto latino (dalla A alla Z) Lettere minuscole dell'alfabeto latino (dalla a alla z) Numeri in base 10 (da 0 a 9) Caratteri non alfanumerici, ad esempio punto esclamativo (!), dollaro ($), simbolo di cancelletto (#) o percentuale (%). Le password possono contenere fino a 128 caratteri.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	**7**	**3**	**M**	**Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)**	Account amministrativi: Il rinnovo della password è manuale in quanto da questi account dipendono vari servizi critici (esempio: trust di domini…). Viene rinnovata durante le attività di manutenzione. Account user: 
5	**7**	**4**	**M**	**Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).**	Il sistema di autenticazione è configurato per impedire il riutilizzo delle ultime 24 password per tutti gli utenti
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	1 giorno.
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Attività gestita da IT Admin

5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	
5	**10**	**1**	**M**	**Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	**10**	**2**	**M**	**Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	**10**	**3**	**M**	**Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.**	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	**11**	**1**	**M**	**Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.**	Le credenziali amministrative riconducibili a persone fisiche sono custodite e gestite dagli stessi. Le credenziali amministrative sono gestito da un programma disponibile sul server (KeePass) protetto da password custodita in archivio P3. Viene gestito backup su dispositivo USB custodito dal RTG in cassetto chiuso a chiave.
5	**11**	**2**	**M**	**Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.**	Non si utilizzano certificati digitali per l'autenticazione delle utenze amministrative.

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	**1**	**1**	**M**	**Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.**	È installato Symantec Endpoint con gestione centralizzata installato su server cm-server01. Regole e aggiornamenti sono distribuiti in maniera centralizzata.
8	**1**	**2**	**M**	**Installare su tutti i dispositivi firewall ed IPS personali.**	Il firewall di Windows è installato e attivo su tutte le macchine Windows per tutti i profili ad eccezione di quello di dominio. Non sono gestite macchine Linux personali
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	**3**	**1**	**M**	**Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.**	Non è permesso l'uso di dispositivi personali non autorizzati e di dispositivi di cui non si possa imporre il controllo
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	*Per dispositivi esterni si intende PC o portatili non censiti nell'elenco di cui alla misura 1.1.1.*
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	

8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
8	**7**	**1**	**M**	**Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro. È stata impostata una regola nella politica predefinita di dominio. 
8	**7**	**2**	**M**	**Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**7**	**3**	**M**	**Disattivare l'apertura automatica dei messaggi di posta elettronica.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**7**	**4**	**M**	**Disattivare l'anteprima automatica dei contenuti dei file.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	**8**	**1**	**M**	**Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro. Configurazione sistema antivirus
8	**9**	**1**	**M**	**Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.**	Il sistema di posta elettronica è configurato in tal senso. L'ente utilizza Icewarp Mail Server. I messaggi vengono controllati dal sistema integrato di antivirus e antispam.
8	**9**	**2**	**M**	**Filtrare il contenuto del traffico web.**	Il network del Comune è dotato di firewall Watchguard M370 con applicazione regole e filtri operativi su tutto il traffico in uscita (personalizzato e misurato per tipo di traffico) ed entrata di: - Antivirus - Intrusion Detection e Prevention - Antispam - Content Filter - Sandbox - Ransomware protection - Application control - Botnet protection

					- Reputation enable defence Il firewall regola anche il traffico tra le subnet presenti (castello, biblioteca, telecamere polizia, comune) Attivo abbonamento con scadenza a fine dicembre 2021
8	**9**	**3**	**M**	**Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).**	Sono utilizzati gli strumenti indicati in ABSC_8.9.1 e ABSC_8.9.2
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	**1**	**1**	**M**	**Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.**	Il sistema informatico dell'ente è strutturato con server virtuali. Attraverso un software specifico vengono copiati tutti i server in uso tutti i giorni, su apparato NAS presente nella stessa stanza Sono conservate copie per 14 giorni. Una mail viene inviata con l'esito quotidiano Le configurazioni degli altri apparati sono in acquisizione. Un altro job di backup viene effettuato su NAS remoto posizionato in biblioteca con conservazione annuaòe
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare il sistema operativo, le applicazioni software e la parte dati.	La copia riguarda l'intero server. In questo modo è possibile ripristinare l'intera VM o il singolo/i file/s
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	

10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Sono pianificate almeno due volte all'anno, utilizzando risorse tecniche messe a disposizione da IT Admin
10	**3**	**1**	**M**	**Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso il sistema di backup. Più specificatamente… I server sono collocati al piano terreno. L'unità di backup è collocata nella medesima stanza. Altra unità di backup è posizionata in biblioteca, in stabile separato dal CED. Si sta implementando un sistema di trasferimento delle copie, criptate, in cloud.
10	**4**	**1**	**M**	**Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.**	E' stata data disposizione agli amministratori di sistema di configurare in tal senso il sistema di backup. Più specificatamente… L'apparecchiatura di backup (NAS) pur essendo collegata fisicamente ella stessa rete è accessibile esclusivamente con credenziali configurate ad hoc per il sistema di backup

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	**1**	**1**	**M**	**Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica**	L'analisi dei livelli particolari di riservatezza è implementata attraverso la compartimentazione dei dati in cartelle il cui accesso è regolato da specifici criteri di accesso (ACL). Il Comune ha rilevato i seguenti ambiti di riservatezza che richiedono crittografia dei dati che è stata realizzata crittografando il volume che contiene le relative cartelle: al momento non sono rilevati. Gli utilizzatori di device mobili hanno istruzione di non memorizzare dati il locale.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	

13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni.	
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	*(ad es. tutti i dati sensibili e giudiziari – vedi Codice privay, TSO, …)* *TUTTI i portatili dovrebbero essere configurati per la crittografia dei file delle cartelle personali.*
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
13	**8**	**1**	**M**	**Bloccare il traffico da e verso url presenti in una blacklist.**	Vedi misura 8.9.2
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	

PIRAS STUDIO

Account utente amministrazione dominio

Dominio : ComuneMalcesine

Nome	Nome dominio	Ora creazione	Nome completo	ID e-mail
Administrator	comunemalcesine.local	gio, 30 gen 2014 14:49:36 +0100	Administrator	-
AuthAdmin	comunemalcesine.local	lun, 11 dic 2017 15:55:53 +0100	Authentication Administrator	-
riccardo.piras	comunemalcesine.local	lun, 11 dic 2017 15:52:34 +0100	Riccardo Piras - GTFH	-
roberto.gasperi	comunemalcesine.local	lun, 11 dic 2017 15:52:13 +0100	Roberto Gasperi - GTFH	-
superandrea	comunemalcesine.local	gio, 12 feb 2015 17:07:08 +0100	Super Andrea - Amministratore - Comune di Malcesine	-

SPICEWORKS

Comune di Malcesine: Nas

Storage (2 items)

Name	Model	Description	Serial Number	Location
cm-qnap		Nas Principale	auto-1576790004.308585-6dccb	Ced
cm-qnapbiblio	TS-469 Pro	Linux TS-469 4.3.4	Q138I05494	Biblioteca

PIRAS STUDIO

SPICEWORKS

Comune di Malcesine: Network

Network Devices (8 items)

Name	Description	Serial Number	Location
HP Procurve 2510g-48	HP ProCurve J9280A Switch 2510G-48	CN141DG1HH	Ced
HP Procurve 2510g-48	HP ProCurve J9280A Switch 2510G-48	CN024DG0ST	Piano
HP Procurve 4104gl	HP J4887A ProCurve Switch 4104GL	SG442AD018	Polizia
Microtik	Microtik	D4CA6D8FE6B2	
Netgear Fs728tp	Netgear FS728TPv2	2F431B54008C1	Ced
Netgear Fs728tp	Netgear FS728TPv2	2F431B5P00917	Piano
Watchguard M370 firewall	Watchguard M370	907FDC7A1E	Ced
ZyXEL gs1900	ZyXEL GS1900-24HP	S142L31003505	Biblioteca

PIRAS STUDIO

SPICEWORKS

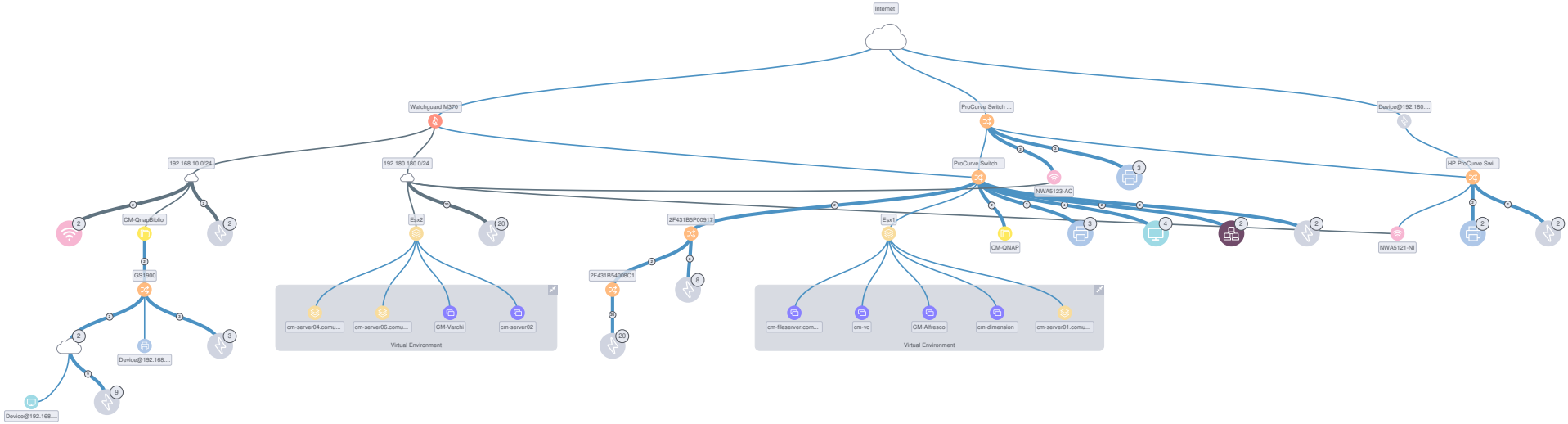
Comune di Malcesine: Server

Phisical and virtual servers (8 items)

Name	Device Type	Description	Is Virtual Machine?	IP Address
cm-fileserver	Server	Server dati, posta, Civilia	Yes	192.180.180.51
cm-server01	Server	Derver DC, Pbx, Antivirus	Yes	192.180.180.1
cm-server02	Server	Server Oracle	Yes	192.180.180.2
cm-server04	Server	Server Concilia	Yes	192.180.180.4
cm-server06	Server	Server Rdp	Yes	192.180.180.6
cm-server07	Server	Server Folium	Yes	192.180.180.7
cm-vc	Server	Server servizi e backup	Yes	192.180.180.20
VM	Server	Unix Computer	Yes	192.180.180.8

PIRAS STUDIO

COMUNE DI MALCESINE TOPOLOGY



PIRAS STUDIO

COMUNE DI MALCESINE

CONFIGURAZIONE REGOLE FIREWALL REV. 1 10/12/2019

Studio Piras S.a.s. – via al Desert, 2 – 38122 TRENTO
tel. +390461390902 +3904611933333
mail: info@studiopiras.net web: www.studiopiras.net

PIRAS STUDIO

Order	Action	Policy Name	Policy Type	From	To	Port	PBR	SD-WAN	App Contro
1		Gestione_CRM	Any	Pc_Gestione_CRM	TelecamerePolizia	any			None
2		POP3	POP3	Any-Trusted	Any-External	tcp:110		Eolo	Global
3		Dimension_to_Fir...	TCP-UDP	192.180.180.9	Firebox	tcp:0 (Any) udp:0 (Any)			None
4		IMAP-Dedagroup	IMAP	Any-Trusted	Any-External	tcp:143		Eolo	Global
5		FTP	FTP	Any-Trusted, Any-...	Any-External	tcp:21		Eolo	Global
6		Auvik_Ports	Auvik_Ports	192.180.180.20	Any-External	tcp:21 udp:21 tcp:69 udp:69		Eolo	None
7		Out_no_proxy_Ht...	Http e Https	Any-Trusted	Siti permessi - No proxy, *.agenziaentrat...	tcp:80 udp:80 tcp:443 udp:443		Eolo	Global
8		out_8080	out_8080	Any-Trusted	Any-External	tcp:8080		Eolo	Global
9		Servizi_per_Folium	Servizi_per_Foli...	Server_Folium	Any-External	tcp:995 udp:995 udp:465 tcp:...		Eolo	Global
10		Affrancatrice	Http e Https	Affrancatrice, Pc_...	Any-External	tcp:80 udp:80 tcp:443 udp:443		Eolo	None
11		Porta_Varchi_SSH	Porta_Varchi_S...	82.185.149.13	88.149.221.100 --> 192.180.180.8 : 22	tcp:10422 udp:10422			None
12		Porta_Varchi_est...	Porta_Varchi_e...	Any-External	88.149.221.100 --> 192.180.180.8 : 21	tcp:10421 udp:10421			None
13		Parcheggio_statu...	Parcheggio_stat...	Any-External	None	tcp:6502 udp:6502 udp:5900 ...			None
14		In_HTTPS_posta	HTTPS	Any-External	88.149.221.98 --> 192.180.180.51, 88.1...	tcp:443			None
15		Certificata	Certificata	Any-Trusted	Any-External	tcp:465 tcp:993		Eolo	Global
16		HTTP-Biblioteca	HTTP-proxy	Biblioteca, giugio (c...	Any-External	tcp:80		Eolo	Global
17		IMAP-proxy	IMAP-proxy	Any-Trusted	Any-External	tcp:143		Eolo	Global
18		HTTP-Utenze_Am...	HTTP-proxy	G-Admins (comune...	Any-External	tcp:80		Eolo	Global
19		HTTP-proxy-No-...	HTTP-proxy	Pc_Ezio, Pc Romani...	Any-External	tcp:80		Eolo	Global
20		HTTP-proxy	HTTP-proxy	Any-Trusted, Ospiti...	Any-External	tcp:80		Eolo	Global
21		HTTPS-proxy.1	HTTPS-proxy	Biblioteca, giugio (c...	Any-External	tcp:443		Eolo	Global
22		HTTPS-proxy-No...	HTTPS-proxy	Pc_Ezio, Pc Romani...	Any-External	tcp:443		Eolo	Global
23		HTTPS-Utenze_A...	HTTPS-proxy	G-Admins (comune...	Any-External	tcp:443		Eolo	Global
24		HTTPS-proxy	HTTPS-proxy	Any-Trusted, Ospiti...	Any-External	tcp:443		Eolo	Global
25		Porta_Cartelloni_...	Porta_Cartelloni...	Any-External	88.149.221.99 --> 192.180.180.200	tcp:9016 udp:9016 tcp:9524 ...			None
26		POP3-proxy	POP3-proxy	192.180.180.51, A...	Any-External	tcp:110		Eolo	Global
27		SNMP	SNMP	192.180.180.20	Firebox	udp:161			None
28		POP3s	POP3s	Any-Trusted, Any-...	Any-External	tcp:995		Eolo	Global
29		SMTP-proxy	SMTP-proxy	Ospiti, Any-Trusted...	Any-External	tcp:25		Eolo	Global
30		SMTPS	SMTPS	Any-Trusted, Any-...	Any-External	tcp:465		Eolo	Global
31		Auvik_Scan_Net...	Any	192.180.180.20	Biblioteca, Ospiti, TelecamerePolizia, Ca...	any			None
32		Porta_LettoreCart...	Porta_LettoreCa...	Any-Trusted	Any-External	tcp:1005 udp:1005		Eolo	Global
33		WatchGuard Web...	WG-Fireware-X...	Any-Trusted, Any-...	Firebox	tcp:8080			None
34		Ping	Ping	Any-Trusted, Any-...	Any	icmp (type: 8, code: 255)			Global
35		Porte_Ministero_CIE	Porte_Ministero...	Postazione_CIE	Any-External	tcp:8442-8443 udp:8442-8443		Eolo	None
36		DNS	DNS	CM-SERVER01	Any-External	tcp:53 udp:53		Eolo	Global
37		VPN_Software_T...	VPN_Software_...	Any-Trusted	VPN_Turismo_IP	udp:1194		Eolo	None
38		Rete_Polizia_vs_r...	Pool_porte_tele...	TelecamerePolizia	Castello	tcp:80 tcp:6036			None
39		In_Pool_porte_tel...	Pool_porte_tele...	Any-External	88.149.221.99 --> 192.168.181.200	tcp:80 tcp:6036			None
40		Porta_Signum_80...	Porta_Signum_8...	Any-External	None	tcp:8081 udp:8081			None
41		WatchGuard	WG-Firebox-Mgmt	Any-Trusted, 88.14...	Firebox	tcp:4105 tcp:4117 tcp:4118			None
42		Desktop_Center	Desktop_Center	Any-External	88.149.221.102 --> 192.180.180.1	tcp:8383 udp:8383			None
43		Porte_Telecamer...	Porte_Telecame...	Any-External	88.149.221.98 --> 192.168.135.150	tcp:6036 tcp:80 udp:80 udp:6...			None
44		Porte_Telecamer...	Porte_Telecame...	Any-External	88.149.221.98 --> 192.168.135.100	tcp:3001 udp:3001 tcp:5005 ...			None
45		Pool_porte_teleca...	Pool_porte_tele...	Any-External	88.149.221.98 --> 192.168.135.10	tcp:2101 udp:2101 udp:21 tc...			None
46		Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5941 udp:5941			None
47		Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5942 udp:5942			None
48		Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5940 udp:5940			None
49		Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5945 udp:5945			None
50		IN_IMAP-proxy	IMAP-proxy	Any-External	88.149.221.98 --> 192.180.180.51, 88.1...	tcp:143 tcp:993 (tls)			None
51		Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5946 udp:5946			None
52		Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5947 udp:5947			None

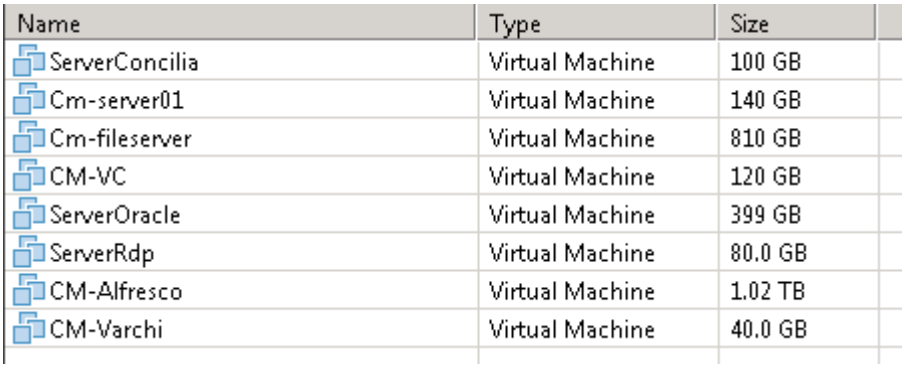
53	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5948 udp:5948		None
54	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5933 udp:5933		None
55	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5939 udp:5939		None
56	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5937 udp:5937		None
57	Assistenza_Cass...	Assistenza_Ca...	Any-External	88.149.221.102 --> 192.168.181.160	tcp:6502 udp:6502		None
58	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5931 udp:5931		None
59	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5936 udp:5936		None
60	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5935 udp:5935		None
61	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5934 udp:5934		None
62	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5938 udp:5938		None
63	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5932 udp:5932		None
64	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5930 udp:5930		None
65	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5926 udp:5926		None
66	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5927 udp:5927		None
67	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5929 udp:5929		None
68	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5925 udp:5925		None
69	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5928 udp:5928		None
70	NTP	NTP	Any-Trusted	Any-External	tcp:123 udp:123	Eolo	Global
71	OUT_Porte_SIP_3...	Porte_SIP_3cx	CM-SERVER01	Any-External	tcp:5060 udp:5060 udp:5061 ...	Eolo	Global
72	Porte_SIP_3cx	Porte_SIP_3cx	Any-External	88.149.221.100 --> 192.180.180.1	tcp:5060 udp:5060 udp:5061 ...		None
73	OUT_RDP	RDP	Any-Trusted	Any-External	tcp:3389	Eolo	None
74	Outgoing	TCP-UDP	TelecamerePolizia, ...	Any-External	tcp:0 (Any) udp:0 (Any)	Eolo	None
75	Parcheggio224	Parcheggio224	Any-External	None	tcp:5924 udp:5924		None
76	ComunevsCastello	Any	Lan_Comune	Castello	any		None
77	Comune_to_Telec...	Any	Lan_Comune	TelecamerePolizia	any		None
78	Biblioteca_to_Co...	Any	Biblioteca	Lan_Comune	any		None
79	Traffico_per_bibli...	Any	Lan_Comune	Biblioteca	any		None
80	Telecamere_to_C...	Any	TelecamerePolizia	Lan_Comune	any		None
81	Allow L2TP-Users	Any	L2TP-Users (Any)	Any	any		None
82	BOVPN-Allow.out	Any	Any	Gtfh	any		None
83	BOVPN-Allow.in	Any	Gtfh	Any	any		None
84	WatchGuard Certi...	WG-Cert-Portal	Any-Trusted, Any-...	Firebox	tcp:4126		None
85	WatchGuard L2TP	L2TP	L2TP-IPSec	Firebox	udp:1701		None
86	WatchGuard Aut...	WG-Auth	Any-Trusted, Any-...	Firebox	tcp:4100		None
87	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5920 udp:5920		None
88	Vnc_parcheggio2...	Vnc_parcheggi...	Any-External	None	tcp:5922 udp:5922		None
89	Vnc_parcheggio2...	Vnc_parcheggi...	Any-External	None	tcp:5921 udp:5921		None
90	Vnc_Parcheggio2...	Vnc_Parcheggi...	Any-External	None	tcp:5923 udp:5923		None
91	SSH	SSH	92.242.173.1-92.24...	88.149.221.102 --> 192.180.180.7	tcp:22		None
92	POP3-proxy.1	POP3-proxy	Server_Folium	Any-Trusted	tcp:110 tcp:995 (tls)		Global
93	IN_Folium_9444	Folium_9444	Any-External	None	tcp:9444 udp:9444		None

COMUNE DI MALCESINE

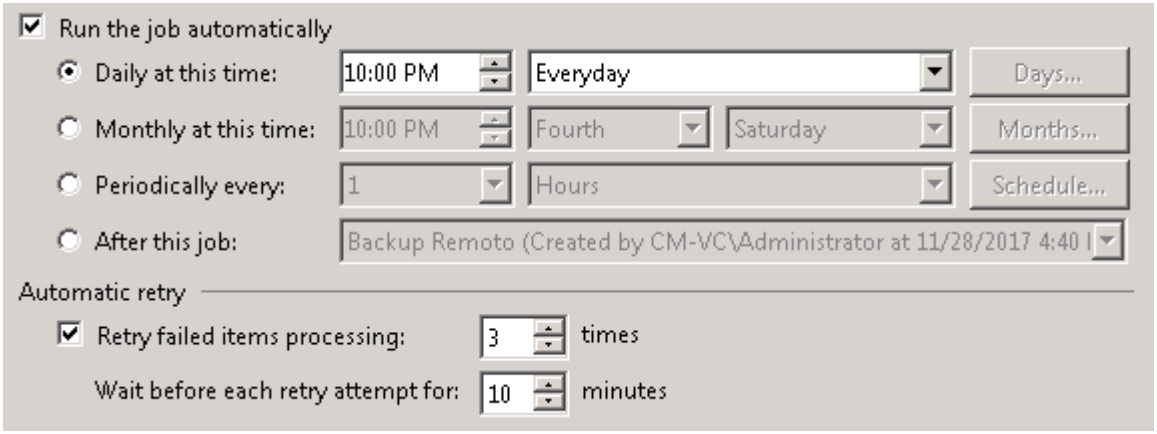
CONFIGURAZIONE BACKUP
REV. 1
10/12/2019

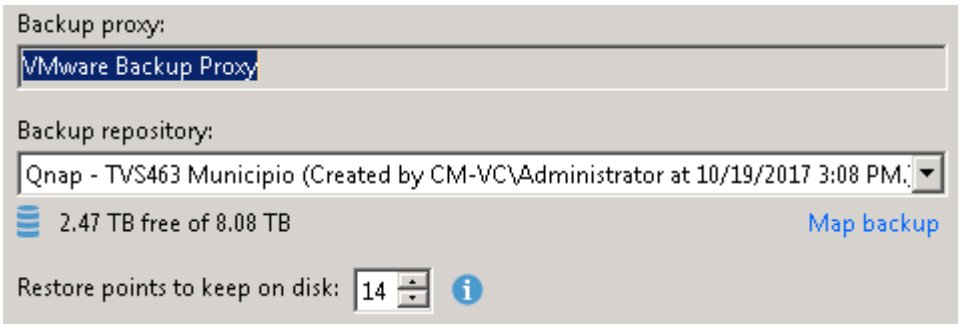
Studio Piras S.a.s. – via al Desert, 2 – 38122 TRENTO
tel. +390461390902 +3904611933333
mail: info@studiopiras.net web: www.studiopiras.net

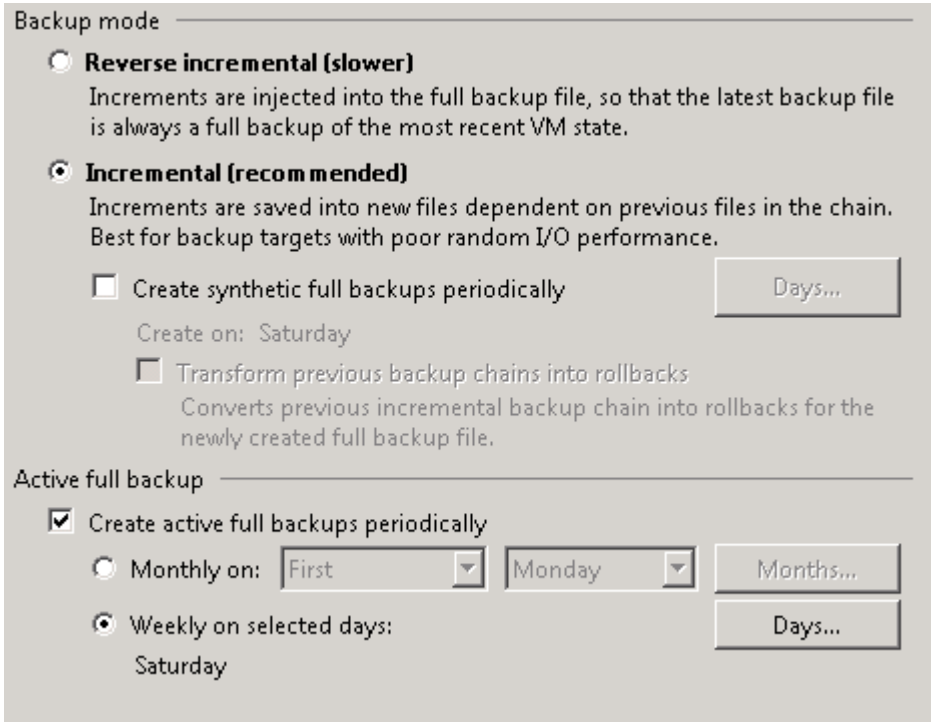
Backup quotidiano su dispositivo QNAP presente nel CED del comune con le seguenti impostazioni:

- Server inclusi:
  - 

Name	Type	Size
ServerConcilia	Virtual Machine	100 GB
Cm-server01	Virtual Machine	140 GB
Cm-fileserver	Virtual Machine	810 GB
CM-VC	Virtual Machine	120 GB
ServerOracle	Virtual Machine	399 GB
ServerRdp	Virtual Machine	80.0 GB
CM-Alfresco	Virtual Machine	1.02 TB
CM-Varchi	Virtual Machine	40.0 GB

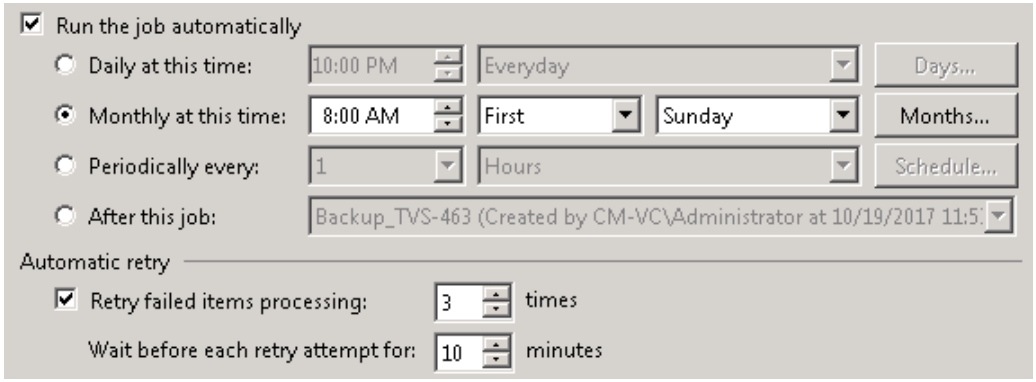
- Schedulazione quotidiana alle 22.00:
  - 

- Retention di 14 giorni:
  - 

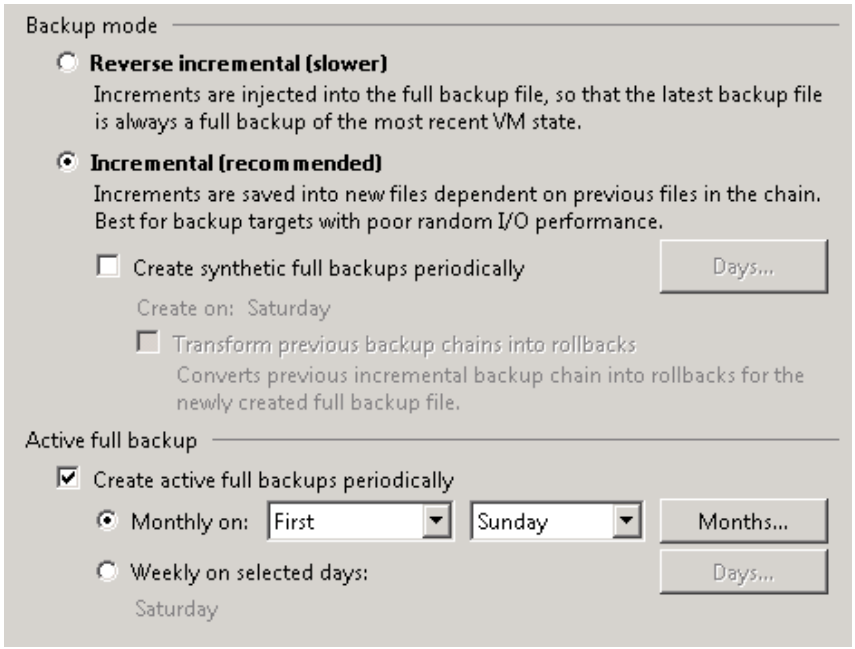
- Tipo di backup, incrementale con full una volta a settimana, il sabato:
  - 

Backup remoto mensile a scopo di disaster recovery su dispositivo QNAP presente presso la Biblioteca

- Server inclusi:
Name	Type	Size
ServerConcilia	Virtual Machine	100 GB
Cm-server01	Virtual Machine	140 GB
Cm-fileserver	Virtual Machine	810 GB
CM-VC	Virtual Machine	120 GB
ServerOracle	Virtual Machine	399 GB
ServerRdp	Virtual Machine	80.0 GB
CM-Alfresco	Virtual Machine	1.02 TB
CM-Varchi	Virtual Machine	40.0 GB

- Schedulazione, mensile la prima domenica:
  - 

- Retention, 12 mesi:
  - 

- Tipo di backup, full mensile:
  - 

Notifiche, dopo l’esecuzione di ogni Job di backup le notifiche del risultato vengono mandate agli indirizzi mail:

romani.andrea@comunemalcesine.it

support@studiopiras.net