COMUNE DI ITTIRI

(PROVINCIA DI SASSARI)

sede legale: Via San Francesco n°1 Ittiri(SS)
C.F. 00367560901 - Tel. **079445200** fax 079445240
Sito Internet: www.comune.ittiri.ss.it

RELAZIONE

TECNICO ILLUSTRATIVA

Sommario

0. - Premessa

La presente relazione fornisce tutte le specifiche dell'impianto di rete informatico presente all'interno delle sedi del Comune di Ittiri, ivi compreso il sistema di approvvigionamento energetico ridondato della Sala Server, con particolare riferimento alle misure minime di sicurezza informatica dell'AgID, di cui alla Circolare n. 2 del 18 Aprile 2019, che sono state adottate dall'ente con Deliberazione di Giunta Comunale n 56 del 14 Marzo 2018. Le stesse sono da intendere come strumento di valutazione per contrastare le minacce più comuni e frequenti a cui sono soggetti i sistemi informatici della PA, e saranno altresì vagliate, nel dettaglio, per identificare eventuali rischi, anche residui, con indicazione delle misure di adeguamento scelte o da scegliere, al fine della corretta efficienza e sicurezza della rete, sia in termini pratici e funzionali, che in termini di legge.

1. – Descrizione nuova Rete Comunale.

L'attuale cablaggio di rete dell'ente è distribuito nelle sedi sotto elencate attraverso un collegamento interno in fibra ottica a velocità 10Gb:

a) sede centrale del Comune di Ittiri sita in Via San Francesco 1;
b) sede decentrata Settore Tecnico Manutentivo sita in Vicolo Marini 1;
c) sede decentrata Settore Anagrafe e Tributi sita in Vicolo Marini 8;

Esso comprendente l'insieme di tutti i componenti necessari (cavi, canalizzazioni, terminazioni, nodi di permutazione, ecc.) utili a garantire la corretta trasmissione dei dati da e per ogni Postazione di Lavoro (PDL). La struttura di rete, si basa sul principio fondamentale quale quello legato alla delocalizzazione delle risorse, mediante l'installazione, per ogni piano, di un armadio Rack dotato di Switch (Multiplatore) 10/10/1000 a 24 porte, pannello di permutazione, striscia di alimentazione e gruppo di continuità, interconnesso al CED mediante fibra ottica 10Gb. I cavi e le prese di rete sono costruite con materiali di categoria 6, e seguono una architettura a stella e sottostella che presenta degli assoluti vantaggi, primo fra i quali l'eliminazione dei punti di collisione rappresentati dalle dorsali da 100Mb precedentemente utilizzate, verso una velocità di dorsale da 10 Gb, che offre delle ottime prestazioni di implementazione soprattutto in chiave futura. Un secondo vantaggio è rappresentato dalla suddivisione del carico di lavoro su un totale di n. 7 Switch anziché essere concentrato su uno unico, riducendo al minimo i rischi di blocco totale della rete. La **figura 1** offre un esempio di schema logico dell'attuale configurazione della rete. La maggiore scalabilità e modularità del nuovo impianto inoltre, è volta a facilitare i lavori di manutenzione e di creazione di nuovi punti rete.

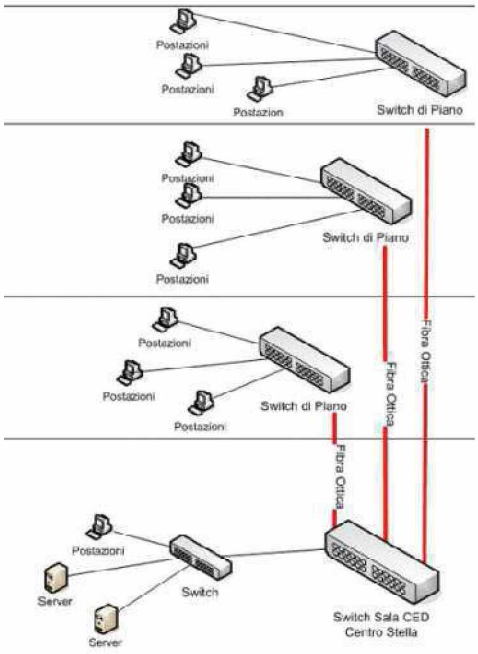

Figura 1

Tutto l'impianto di rete informatico prevede un:

- **Cablaggio Orizzontale** che partendo dall'Armadio a Rack, sito in un locale tecnico di piano, raggiunge in maniera stellare la postazione di lavoro mediante connettori modulari di tipo RJ45, con pannelli di permutazione in Cat. 6, placche, frutti e bretelle di connessione, anch'esse della stessa categoria. Nei cavi di rete viene distribuito sia il servizio di fonia che quello dati, con possibilità di interconnessione anche attraverso una rete Wifi (una per piano) i cui accessi sono monitorati giornalmente dall'amministratore di sistema. Tutti i componenti, pannelli di permutazione, cavi di distribuzione orizzontale (Cavo UTP in rame Cat6 con guaina LSZH), Patch Cord (bretelle di permutazione lato armadio) e Work Area Cable (bretelle lato postazione di lavoro), sono conformi agli standard EIA/TIA 568-B.2-1 e ISO/IEC 11801. Un esempio grafico della struttura logica è presente in **figura 2**;

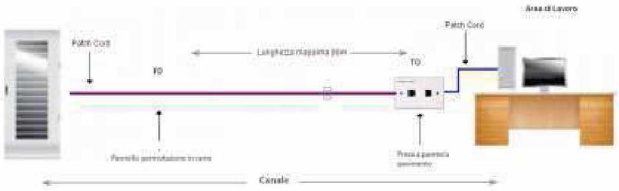

Figura 2

- **Cablaggio di Dorsale:**Il cablaggio di dorsale estende il raccordo tra l'armadio principale di edificio e l'armadio di piano. Anch'esso prevede una Dorsale Dati (in fibra ottica) e una Dorsale Fonia (con cavi multi coppia in rame). Le dorsali dati sono realizzate con cavi in fibra ottica multimodale a garanzia dei collegamenti tra gli apparati di centro stella e gli apparati di distribuzione di piano. Sono state previste, per tenere conto di possibili sviluppi futuri della rete, eventuali fibre di scorta quale ridondanza o di backup. Il tratto in fibra dall'armadio di centro stella all'armadio di piano è realizzato impiegando un cavo senza interruzioni, di tipo "loose" con filamenti ottici di tipo (requisito minimo) multimodale 50/125 μm tipo om3, con larghezza di banda maggiorata per supportare applicazioni da 1Gbps a 10 Gbps Ethernet. Il cavo utilizzato è conforme alle specifiche di sicurezza dettate dalle normative CEI, relative agli edifici ad alta densità di popolazione e

alla protezione da pericolo di incendio. Tutta la rete è rispondente agli standard d'interconnessione emanati dai seguenti organismi:

- TIA/EIA: Telecomunication Industries Association / Eletronic Industries Association;
- ISO/IEC: International Standard Organization / Internation Electrotechnical Commission;
- ANSI: American National Standard Institute;

- **Armadi di Piano e di Centro Stella:** Gliarmadi di distribuzione di Piano sono costituiti da una struttura in lamiera d'acciaio passivata, pressopiegata ed elettrosaldata, basati sulla tecnica Rack 19", corredati di due montanti laterali completamente perforati (doppia foratura) con passo multiplo di 1U. La **figura3**, rappresenta fedelmente la tipologia di armadi di installati, ognuno dei quali forniti di adeguati UPS. L'armadio di centro stella, già presente all'interno della Sala CED, è stato completamente ristrutturato e riqualificato energeticamente con l'installazione di un adeguato UPS. Su ognuno degli Armadi di Piano e di Centro Stella è affisso un documento con la Mappatura e Numerazione delle Prese di rete, con la specifica di alcune informazioni come il Nr. di Presa, Nome e Cognome Utilizzatore, eventuali Note aggiuntive. Un esempio di documento si riporta in **figura4**;

Figura 3

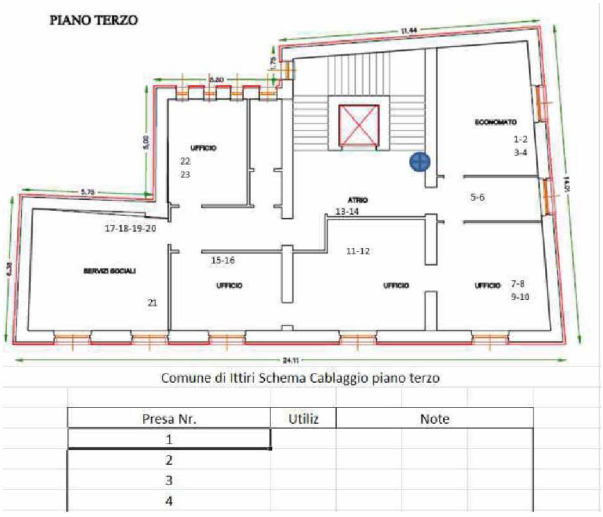

Figura 4

2. – Descrizione Sala CED e Apparati Informatici del Comune di Ittiri.

La Sala CED dell'Ente è sita nei locali di Via San Francesco, 1 in Ittiri, ed al proprio interno si trovano i sotto elencati apparati Server e di gestione attiva e passiva di rete, i quali sono serviti da un nuovo sistema di approvvigionamento energetico ridondato attraverso 2 linee energetiche separate e doppio UPS (Figura 5 e 6):

- Nr. 1 Router Huawei dedicato al collegamento verso internet con banda fino a 20 Mb;
- Nr. 1 Router Box 4G di Backup dedicato al collegamento ad internet con banda fino a 100 Mb;
- Nr. 1 Router Huawei dedicato al centralino virtuale con tecnologia Voip con banda fino a 4 Mb;
- Nr. 1 Router Box 4G di Backup dedicato al centralino virtuale con tecnologia Voip fino a 4 Mb;
- Nr. 1 Server HP-DL380 G7 con Sistema Operativo ESXI e Nr. 5 Macchine Virtuali al suo interno, e caratteristiche Hardware: CPU 4x2.53 GHz, RAM 28 GByte, HDD 3 TByte in configurazione RAID 5 (6 Hard Disk di cui 2 Hot Spare);

- Nr. 1 Server HP-DL380 G9 con Sistema Operativo ESXI e Nr. 5 Macchine Virtuali al suo interno e caratteristiche Hardware: CPU 6x1.90 GHz, RAM 48 GByte, HDD 5.5 TByte in configurazione RAID 5(4 Hard Disk di cui 1 Hot Spare);
- Nr. 1 Nas Synology RAID 5 utilizzato per il Backup delle Macchine Virtuali e Dati dell'applicativo
- interno di Gestione Comunale Sicraweb;
- Nr. 1 Nas QNAP RAID 1-0 utilizzato per il Backup delle cartelle di Rete condivise;
- Nr. 1 Firewall di rete Anti Intrusione;

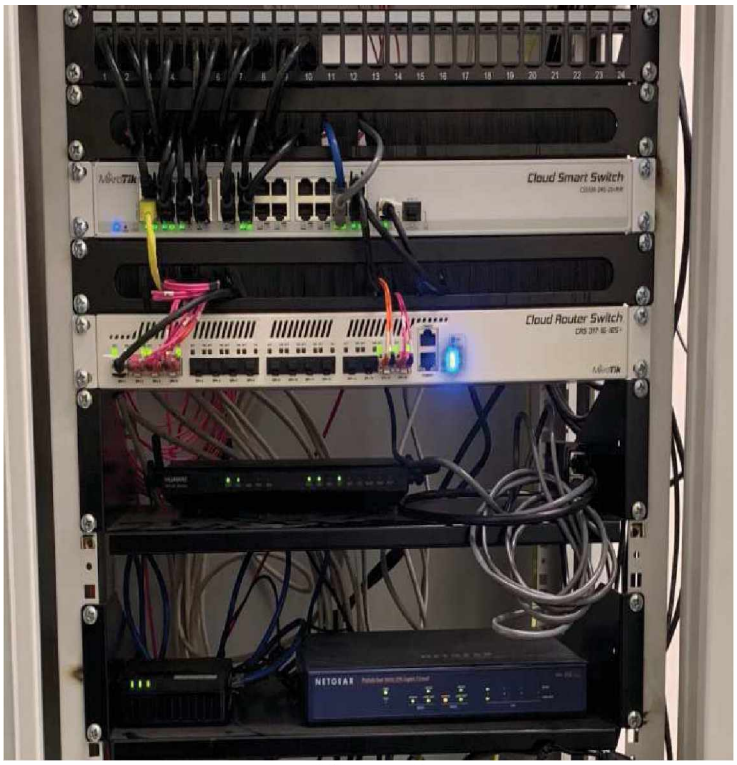

Figura 5

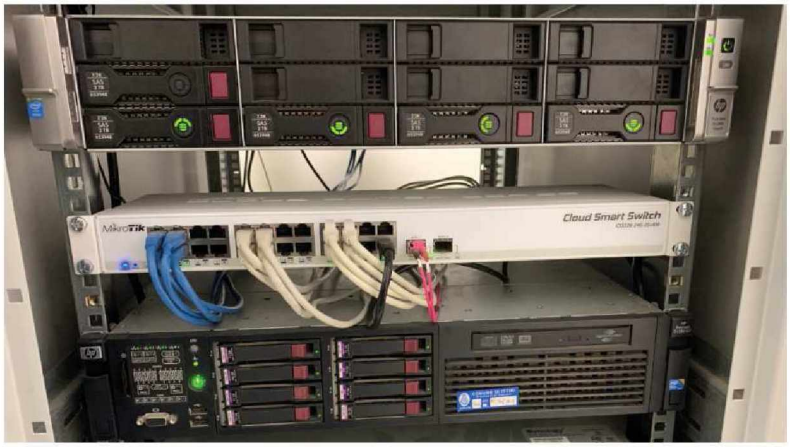

Figura 6

I due Router Huawei in dotazione all'ente si occupano di fornire la connettività internet e di fonia per il centralino virtuale Voip. Entrambi sono muniti con Box 4G esterno che, attraverso l'ausilio di una SIM dati, fornisce la continuità del servizio di connettività internet e di fonia qualora le linee portanti principali dovessero venire meno per eventuali disservizi tecnici dell'operatore. In Sala Server sono installati Nr. 2 Server HP DL380 che ospitano le Macchine Virtuali con a bordo tutti i Software che l'ente utilizza giornalmente per la sua attività amministrativa e di gestione. In

particolare, all'interno del Server HP-DL380 G7 con Sistema Operativo ESXI sono presenti le Macchine Virtuali di Figura 7:

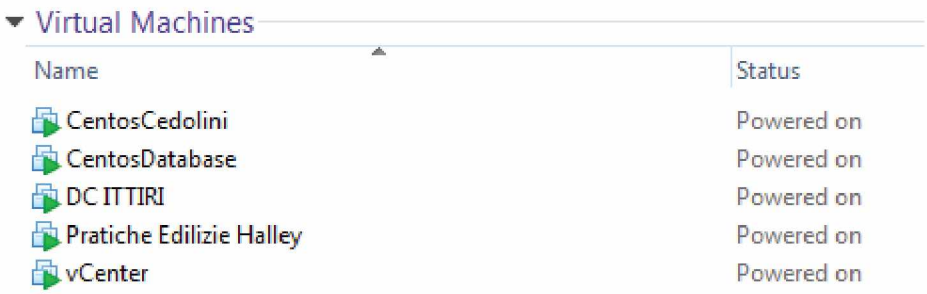

Figura 7

1. La Macchina Virtuale "**Centos Cedolini"** si occuperà a breve, con un opportuno software installato e configurato, della gestione delle Presenze/Assenze del dipendenti comunali, i quali potranno gestire in completa autonomia, attraverso un "Portale Dipendenti Online", tutte le loro Informazioni Giuridiche, come ad esempio scaricare le CU, le Buste paga e Richiedere le Ferie e/o Permessi. Tale software sarà installato e configurato dalla Maggioli Spa;
2. La Macchina Virtuale "**Centos Database"** si occupa della gestione del Database del software "Sicraweb". Tale Software è utilizzato per la completa gestione informatica di tutte le procedure amministrative, come il Protocollo Informatico, le Delibere, le Determine, le Pubblicazioni, la Gestione di Anagrafe Finanziaria dell'ente ecc....Il Software è di proprietà di Maggioli Spa;
3. La Macchina Virtuale "**DC ITTIRI"**funge da Domain controller (DC) che, nell'ambito delle reti gestite con Microsoft Windows Server System, è un server in grado di gestire richieste di autenticazione per la sicurezza (login, controllo dei permessi, ecc.) e organizzare la struttura del Dominio in termini di Utenti, Gruppi e Risorse di rete, fornendo dunque un servizio di Active Directory Service. Il Dominio attualmente installato è di tipo "Primary Domain Controller", ma non si esclude in un prossimo futuro, la possibilità di avere un duplicato in modo che, in caso di Fault del Primary Domain Controller, intervenga autonomamente come Secondary Domain Controller. Il DC è stato realizzato con Licenza Windows Server 2012 Rok;
4. La Macchina Virtuale "**Pratiche Edilizie Halley"**si occupa della gestione del software di Pratiche Edilizie in uso all'ente, il quale è fornito dalla Halley Sardegna. Anche se la Macchina Virtuale è presente in rete, solamente un unico utente autorizzato ha accesso alla lavorazione delle informazioni in essa contenute, essendo protetto da Username e Password che solamente lo stesso utente conosce;
5. La Macchina Virtuale "**VCenter"**, si dovrebbe occupare della gestione "Unica" delle Macchine Virtuali di entrambe i Server HP-DL380. In particolare il VCenter in modalità Appliance, darebbe la possibilità di creare un unico "Cluster" dei due Server, in modo da avere una panoramica completa di tutte le risorse, sia in termini software che di hardware di entrambe i Server HP-DL380. Tale Macchina Virtuale risulta in fase testing/configurazione da parte dell'amministratore di sistema;

Viene ora analizzato l'interno del Server HP-DL380 G9 con Sistema Operativo ESXI e le sue Macchine Virtuali, la cui lista è presente in Figura 8:

Figura 8

1. La Macchina Virtuale "**Centos Applicativo"** si occupa della gestione dei dati dell' Applicativo Software "Sicraweb". Come già spiegato precedentemente, questo Software è utilizzato per la completa gestione informatica di tutte le procedure amministrative, come il Protocollo Informatico, le Delibere, le Determine, le Pubblicazioni, la Gestione di Anagrafe Finanziaria dell'ente ecc....Il Software è di proprietà di Maggioli Spa;
2. La Macchina Virtuale "**Gestione Presenze"** si occupa della attuale Gestione delle Presenze/Assenze del dipendenti comunali. Questo software, con annessa Macchina Virtuale, sarà di prossima revisione e cessazione a beneficio del nuovo Software di gestione. Attualmente il Software in uso è fornito dalla Kronotech Spa;
3. La Macchina Virtuale "**Intranet - (Windows 7)"**si occupa della gestione del Backup delle Macchine Virtuali attraverso un Software licenziato chiamato "Veem Backup e Replication". Il Software, opportunamente configurato, effettua giornalmente un Backup incrementale all'interno del NAS Synology, e un Backup Completo, una volta al mese, di tutte le Macchine Virtuali presenti all'interno dei Server HP-DL380. E' da sottolineare che, ogni volta che si conclude un Backup, sia in modo positivo che negativo, viene inviata una email all'amministratore di sistema con il report della giornata precedente, in modo da avere tempo di rimediare manualmente in caso di Fault di un qualsiasi Backup. Inoltre, sempre nella Macchina Virtuale "**Intranet - (Windows 7)"**è presente un Server Web che gestisce la Intranet del Comune di Ittiri, dove vengono postate informazioni, link e guide utili all'attività amministrativa di tutti i colleghi. La "Intranet", attraverso una Group Policy configurata all'interno del Domain Controller, è la prima "HomePage" che l'utente visualizza appena apre qualsiasi Browser Web per navigare su internet;
4. La Macchina Virtuale "**Servizio Associato"**si occupa della gestione del Software di Polizia Locale denominato "Concilia", il quale contiene tutti i dati relativamente alle infrazioni commesse dai cittadini del Comune di Ittiri, con possibilità di effettuare, attraverso collegamenti alla MTCT, attraverso la rete e/o attraverso il telefonino/tablet in dotazione, opportunamente configurato, ricerche per nominativo delle targhe automobilistiche che la Polizia Locale verifica giornalmente. Il Software è di proprietà di Maggioli Spa.
5. La Macchina Virtuale "**Server Ittiri"**ospita un vecchio Sistema Operativo dove sono presenti cartelle di rete ancora in uso da parte dei colleghi. E' in corso la dismissione della stessa appena verranno trasferite le cartelle di rete, ancora utilizzate, verso la nuova destinazione che è stata identificata nel NAS Synology.

Il Nas Synology (figura 9), in configurazione RAID 5 (10 Dischi da 500 GByte e 2 Dischi in Hot Spare), viene utilizzato per il Backup delle Macchine Virtuali e dei Dati dell'applicativo interno di Gestione Comunale "Sicraweb". Il Backup è configurato in modo da rimanere protetto anche in caso di Virus, come ad esempio un attacco di "Cryptolocker", dove è possibile recuperare i dati, eventualmente virati e criptati, semplicemente "ritornando indietro di N giorni, "prima del virus" e procedendo al ripristino. E' in corso la progettazione, da parte dell'amministratore di sistema, di un

Disaster Recovery Delocalizzato in altra Sede Comunale per tenere al sicuro i dati detenuti dall'ente in caso di eventuali danni in Sede Centrale. Nello specifico si sta studiando la possibilità di acquisire un ulteriore NAS Synology da installare in altra sede delocalizzata, configurando in modo da ospitare l'intero Backup;

Figura 9

Il Nas QNAP (Figura 10), in configurazione RAID 1-0 (2 Dischi in Mirroring), viene utilizzato per il Backup delle cartelle di Rete condivise all'interno dell'ente. Anche in questo caso, si sta studiando la possibilità di integrare l'intero contenuto dello stesso, all'interno del NAS Synology (di futura e imminente acquisizione), da installare in altra sede configurandolo in modo da ospitare tutto il Backup presente nella Sede Centrale di Via San Francesco;

Figura 10

Il Firewall di Rete Anti Intrusione (Figura 11), infine, è il dispositivo di difesa perimetrale della rete informatica del Comune di Ittiri, che fornisce una protezione in termini di sicurezza informatica della rete stessa, nonchè l'accesso controllato di tutti i Client ad internet. Di norma, la rete è divisa in due sottoreti: una, detta esterna, è tipicamente una WAN (Wide Area Network) che può comprendere Internet, mentre l'altra interna, detta LAN (Local Area Network), comprende una sezione più o meno grande di un insieme di computer host locali (Client, Stampanti, Scanner, etc...). Non è presente, ma è intenzione dell'ente, una terza sottorete, cosìdetta DMZ (o zona demilitarizzata), adatta a contenere tutti quei sistemi Server che devono essere isolati dalla rete interna, ma che devono comunque essere protetti dal firewall ed essere raggiungibili dall'esterno.

Figura 11

3. – Descrizione del Sistema di Videosorveglianza

Il Sistema di Videosorveglianza dell'ente (Figura 12), è dislocato fisicamente al Piano 1° dei locali di Via San Francesco 1, presso la Sala CED, e si compone dei seguenti Hardware:

- Nr 2 DVR (Registratori con a bordo Nr. 2 Hard Disk della capienza di 1 TByte ciascuno) ai quali sono collegate le telecamere di videosorveglianza analogiche e digitali;
- Nr 2 Tipologie di rete Mesh e Nr. 1 UPS di supporto in caso di problemi di alimentazione elettrica;

Figura 12

Il Comune di Ittiri possiede una videosorveglianza attiva a controllo del perimetro del Municipio, la quale consiste di Nr. 7 telecamere analogiche collegate ad un DVR. In questi ultimi anni, grazie all'utilizzo di alcuni fondi comunali, si è provveduti a progettare ed installare altre 5 telecamere digitali di nuova generazione a controllo di alcune piazze cittadine e parchi comunali. Il nuovo sistema di videosorveglianza progettato è totalmente scalabile e implementabile in quanto si basa sulla tecnologia HiperLan, la quale, attraverso l'utilizzo di antenne settoriali, connette la stazione centrale (antenna principale installata sul tetto del Municipio), a tutte le postazioni di controllo video. La gestione della videosorveglianza, ivi compresa la visualizzazione e il salvataggio delle immagini e dei video delle telecamere, è stata attribuita, con Deliberazione di Giunta e di Consiglio, al Comandante della Polizia Municipale, il quale, attraverso una postazione di lavoro dedicata e installata presso gli uffici del Settore SPD, gestisce e coordina tutto il sistema. Relativamente al Registro di Trattamento in conformità del GDPR, al punto 16 SPD, sono state specificate tutte le azioni utili e responsabilità relativamente alla videosorveglianza. In particolare, vengono definite le figure che potrebbero accedere al sistema quali:

- Titolare di Posizione Organizzativa del Settore e Responsabile del procedimento;
- Ufficio vigilanza e polizia urbana e Responsabile del procedimento Ufficio Vigilanza Verbali;

- Amministratore di sistema;
- Tirocinanti o studenti in alternanza scuola lavoro;

La conservazione dei dati, delle informazioni e delle immagini raccolte è limitata ai 7 giorni successivi alla registrazione, salvo esigenze di verifica e controllo, come richieste degli organi di Polizia Giudiziaria e dell'autorità giudiziaria. In riguardo alle misure specifiche poste in essere per fronteggiare i rischi di distruzione, perdita, modifica, accesso o divulgazione non autorizzata, la cui efficacia va valutata regolarmente, L'accesso al sistema per la visualizzazione e gestione dei dati viene consentito attraverso l'inserimento di una username e di una password, che viene detenuta esclusivamente dal Comandante della Polizia Locale designato. La rete di videosorveglianza è totalmente scollegata dalla rete internet e, risulta accessibile esclusivamente dalla postazione di gestione installata presso il piano terra del Municipio sito in Via San Francesco 1, negli uffici del Settore Polizia Municipale e Demografico. E' dunque impossibile accedere ai dati della videosorveglianza dall'esterno, a meno di richieste particolari che saranno vagliate di volta in volta al fine di assicurare la corretta gestione e conservazione dei dati presenti.

4. – Descrizione Client del Comune di Ittiri e Sistema di Protezione Antivirus

Le postazioni Client della rete sono all'incirca 50, e si connettono alla rete comunale attraverso un DHCP Server che viene gestito direttamente dal Firewall Netgear. L'accesso alla rete viene abilitato esclusivamente se il MAC Address della postazione richiedente (Indirizzo Fisico della Scheda di rete), è inserito all'interno della sezione "Access MAC Address Granted" del Firewall Netgear.

Nel caso in cui l'indirizzo fisico della postazione non sia presente all'interno della su indicata lista, la stessa non avrà accesso né alla rete locale e internet, né tantomeno ai servizi offerti. All'avvio della postazione viene richiesta un password di accesso che viene aggiornata ogni 90gg dall'utilizzatore della postazione. Solamente l'utilizzatore e l'amministratore di sistema sono a conoscenza della password di accesso alla postazione singola, e in mancanza dell'utilizzatore, qualora si debba utilizzare la postazione, solo l'amministratore di sistema è autorizzato ad accedervi o a far accedere un altro collega autorizzato, avendo cura, una volta concluso l'utilizzo, di provvedere al reset della password di accesso e alla comunicazione della modifica al collega a cui compete l'utilizzo primario della postazione.

Tutte le postazioni della rete informatica hanno Sistema Operativo Windows 7 Professional con software di Office Automation OpenOffice e/o LibreOffice, equipaggiate con Software Antivirus Eset Nod 32, il cui aggiornamento viene gestito direttamente dal Controller di Dominio attraverso un opportuno Agent installato sul Server e sui Client. Esistono anche Nr. due Computer Notebook per uso interno con sistema operativo Windows 7 Professional. Al fine di monitorare eventuali installazioni di software non autorizzato, l'ente ha in dotazione un software di gestione della rete chiamato Desktop Central Manager Engine che viene monitorato mensilmente. Risulta comunque impossibile, da parte dell'utente utilizzatore, installare software a piacimento in quanto la password di abilitazione alle installazioni è di conoscenza esclusiva dell'amministratore di sistema che ne cura l'aggiornamento periodico e la corretta e sicura conservazione in un locare/programma opportunamente protetto.

5. –Linee Guida AgID del Comune di Ittiri, Identificazione rischi, e misure di adeguamento

Le linee guida AGID definiscono degli indicatori denominati Agid Basic Security Control (ABSC) ciascuno dei quali è classificato come misura di sicurezza Minima (M), Standard (S) o Alta (A). In questa sezione saranno vagliati nel dettaglio per cercare di dare una visione il più concreta possibile della situazione in cui si trova la rete informatica del Comune di Ittiri. Saranno altresì

identificati eventuali rischi con indicazione delle misure di sicurezza adottate o da adottare al fine della corretta efficienza e sicurezza della rete, sia in termini pratici e funzionali, che in termini di legge. Si allega a questo documento le misure minime di sicurezza informatica dell'AgID, di cui alla Circolare n. 2 del 18 Aprile 2019, che sono state adottate e opportunamente conservate dall'ente con Deliberazione di Giunta Comunale n 56 del 14 Marzo 2018.

ABSC1: INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso.

L'accesso alla rete da parte dell'utilizzatore viene abilitato esclusivamente se il MAC Address della postazione richiedente (Indirizzo Fisico della Scheda di rete), è inserito all'interno della sezione "Access MAC Address Granted" del Firewall Netgear, il quale, in conformità all'ABSC 1, è anche in grado di tracciare i Log di tutte le operazioni del Server DHCP che fa ottenere l'accesso alla rete comunale a tutte le postazioni. L'amministratore di sistema detiene, nel proprio archivio protetto, un opportuno file excel sempre aggiornato, con indicazione di tutte le informazioni come ad esempio, nome dell'utilizzatore della postazione, caratteristiche hardware e software della postazione, indirizzo ip della postazione, Sistema Operativo e/o eventuale altro hardware detenuto all'interno degli uffici dell'ente. Un esempio non esaustivo del contenuto del file è presente in figura 13.

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Nome	Cognom	Nome Comput	Marca PC	Modello PC	RAM	Marca Moni	Modello Monit	Marca UPS	Marca Stampan	Modello Stampante	Tastie	Moua	Altro
Angelo	Baldinu	PC-S1UT-P1-27	Acer Intel Core I54460	Veritrpo X2631G	4GB	AOC	E2270SW	Atlantis One Power	HP	DESINGER HC PLUS	X	X	Scan Lemark K5150
Gian Luigi	Cossu	PC-S1UT-P1-54	ThinkCentre	Pentium I3	4GB	HannsG	HP227	Atlantis One Power	HP	LASER JET 4 PLUS	X	X	Sopo Epson 2480 Photo
Francesco	Maloni	PC-S1UT-P2-29	Asus	P5KPL-AMSE	4GB	Asus	WW225	Atlantis One Power	PHASER	6110	x	x	
Antonio	Deriu	PC-S1UT-P2-30	ThinkCentre	Pentium I3	4GB	Asus	VW1935	Atlantis One Power	RICOH	AFICIO SPC232DX	x	x	
Giovanni Giacomo	Pisanu	PC-S1UT-P2-31	Acer	Veriton X2631G	4GB	Hannsg	HW1910	Atlantis One Power			x	x	

Figura 13

ABSC 2: INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione.

L'ente ha in dotazione un software di gestione della rete chiamato Desktop Central Manager Engine che viene monitorato e aggiornato mensilmente. Tale software viene utilizzato per inventariare, tracciare, ed eventualmente correggere, tutti i software, autorizzati e non, presenti sulla rete. L'installazione di qualsiasi software è comunque vincolata alla conoscenza della password di abilitazione alle installazioni, la quale conoscenza è di esclusività dell'amministratore di sistema, che ne cura l'aggiornamento periodico e la corretta e sicura conservazione in un locare/programma opportunamente protetto.

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

Istituire, implementare e gestire attivamente (tracciare, segnalare, correggere) la configurazione di sicurezza di laptop, server e workstation utilizzando una gestione della configurazione e una procedura di controllo delle variazioni rigorose, allo scopo di evitare che gli attacchi informatici possano sfruttare le vulnerabilità di servizi e configurazioni.

Tutti i dispositivi autorizzati ad accedere alla rete informatica comunale sono configurati in modo da dover passare obbligatoriamente attraverso l'autenticazione del Controller di Dominio, in modo da verificarne la corretta identità al fine di poter accedere alle risorse della rete stessa. Gli aggiornamenti di sistema, nonché quelli di antivirus, sono gestiti attraverso l'utilizzo di GPO

(Criteri di Gruppo). Le Group Policy Object sono un insieme di regole che controllano l'ambiente di lavoro di tutti gli utenti e dei computer. Forniscono la gestione centralizzata e la configurazione di sistemi operativi, applicazioni e le impostazioni degli utenti in un ambiente Active Directory. In altre parole, le Group Policy in parte controllano ciò che gli utenti possono o non possono fare su un sistema informatico, I criteri di gruppo sono spesso utilizzati per limitare determinate azioni che possono rappresentare potenziali rischi di protezione, ad esempio: per bloccare l'accesso al Task Manager, limitare l'accesso a determinate cartelle, disabilitare il download di file eseguibili, disabilitare l'uso di unità esterne (penne USB, dischi ottici) e così via. Il Firewall di Rete Anti Intrusione (Figura 11), infine, funge da dispositivo di difesa perimetrale della rete informatica del Comune di Ittiri, fornendo una protezione in termini di sicurezza informatica della rete stessa, nonchè l'accesso controllato di tutti i Client ad internet. Lo stesso Firewall, opportunamente configurato, controlla e registra, in file di testo log, eventuali accessi esterni autorizzati che vogliano utilizzare servizi interni all'ente, come ad esempio accesso al software di gestione Sicraweb.

ABSC 4: VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

Acquisire, valutare e intraprendere continuamente azioni in relazione a nuove informazioni allo scopo di individuare vulnerabilità, correggere e minimizzare la finestra di opportunità per gli attacchi informatici.

L'avvento di nuove modalità di attacco informatico, software maligni come virus e troyan etc…, costringono l'ente a porre un occhio di riguardo relativamente a questa problematica. Nonostante l'amministratore di sistema abbia a disposizione strumenti di scansione delle vulnerabilità regolarmente aggiornate, lo stesso, deve essere sempre pronto ad intervenire, anche manualmente, per risolvere eventuali falle che si possano creare da aggiornamenti non correttamente applicati sia a livello di sistema operativo che di antivirus sulle varie postazioni informatiche. Di norma tutte le patch di aggiornamento vengono installate automaticamente attraverso il Server di Dominio. Tutte queste informazioni devono essere presenti all'interno di un documento denominato Piano dei Rischi che non è ancora stato predisposto ma che verrà implementato entro il triennio 2018-2020.

ABSC 5: USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi. Tutto il personale amministrativo deve digitare una password personale per

l'accesso ai sistemi che deve essere cambiata regolarmente ed in modo autonomo dal proprietario. Sono fornite indicazioni a tutti gli utenti per l'utilizzo di password di autenticazioni "forti" che, dato il contesto in cui si opera, si ritiene debbano essere "almeno 8 caratteri di cui uno speciale + 1 numero + una maiuscola" La gestione degli utenti è fatta dall'amministratore di sistema che abiliterà gli utenti su ciascuna postazione client con i relativi permessi di accesso al server, alle applicazioni e alle risorse condivise (spazio disco del server, stampanti di rete, etc.).

In riferimento a tali specifiche si rimanda al documento delle misure minime di sicurezza informatica dell'AgID, di cui alla Circolare n. 2 del 18 Aprile 2019, che sono state adottate e opportunamente conservate dall'ente con Deliberazione di Giunta Comunale n 56 del 14 Marzo 2018.

ABSC 8: DIFESE CONTRO I MALWARE

Controllare l'installazione, la diffusione e l'esecuzione di codice maligno in Diversi punti dell'azienda, ottimizzando al tempo stesso l'utilizzo dell'automazione per consentire il rapido aggiornamento delle difese, la raccolta dei dati e le azioni.

L'ente, al fine di prevenire attacchi informatici attraverso internet, ha in dotazione un Software Antivirus Eset Nod 32 il cui aggiornamento viene gestito direttamente dal Controller di Dominio attraverso un opportuno Agent installato sul Server e sui Client. La verifica degli aggiornamenti delle Licenze e delle scansioni periodiche sono di competenza dell'amministratore di sistema, il quale è chiamato ad intervenire, anche manualmente, al fine di proteggere i dati dell'ente.

ABSC 10: COPIE DI SICUREZZA

Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.

Come già anticipato, nella Macchina Virtuale "**Intranet - (Windows 7)"** è presente un Software licenziato chiamato "Veem Backup e Replication" che si occupa della gestione del Backup delle Macchine Virtuali. Il Backup è pianificato giornalmente ed è di tipo incrementale. L'hardware che contiene la copia di tutti i dati di Backup è il NAS Synology. Ogni volta che si conclude un Backup, sia in modo positivo che negativo, viene inviata una email all'amministratore di sistema con un report dettagliato sul backup appena effetuato, in modo da avere tempo di rimediare manualmente in caso di Fault. Tutti i backup sono conservati all'interno del NAS e non accessibili a meno dell'amministratore, il quale accede quotidianamente per verificarne il corretto salvataggio in caso di messaggi anomali.

Il Backup è configurato in modo da rimanere protetto anche in caso di Virus, come ad esempio un attacco di "Cryptolocker", dove è possibile recuperare i dati, eventualmente virati e criptati, semplicemente "ritornando indietro di N giorni, "prima del virus" e procedendo al ripristino. E' in corso la progettazione, da parte dell'amministratore di sistema, di un Disaster Recovery Delocalizzato in altra Sede Comunale per tenere al sicuro i dati detenuti dall'ente in caso di eventuali danni in Sede Centrale. Nello specifico si sta studiando la possibilità di acquisire un ulteriore NAS Synology da installare in altra sede delocalizzata, configurando in modo da ospitare l'intero Backup;

ABSC 13: PROTEZIONE DEI DATI

Processi interni, strumenti e sistemi necessari per evitare l'esfiltrazione dei dati, mitigarne gli effetti e garantire la riservatezza e l'integrità delle informazioni rilevanti.

In riferimento a questa ultima parte si provvederà quanto prima alla creazione di un Proxy Server in grado di filtrare il traffico http in modo corretto, consentendo l'accesso ai vari siti web attraverso una Whitelist e non consentendolo attraverso una Blacklist.

6. – Fornitori di Servizi e Privacy

Sito Istituzionale Comune di Ittiri

Il sito web, le email e le PEC sono ospitati su hosting server dislocati nei data center italiani di **Aruba S.p.A.**, certificati ai massimi standard (Rating 4) secondo ANSI/TIA 942-A. E' garantito l'accesso remoto tramite adozione diversi protocolli di comunicazione e l'utilizzo di specifiche credenziali di amministratore.

Da parecchi anni Aruba è certificata e rispetta gli standard di sicurezza logica, fisica e organizzativa imposti della certificazione ISO 27001. Oltre a molte altre certificazioni tra cui ISO 9001, ISO 14001, ANSI/TIA 942-A.

I data center di Aruba rappresentano un'eccellenza grazie al massimo della tecnologia, a standard di sicurezza certificati

- **Certificato** **SSL**
  Il protocollo di sicurezza che consente di evitare la divulgazione non autorizzata o l'accesso ai dati personali trasmessi.
- **Backup** **giornaliero**
  Contro il rischio di perdita accidentale dei dati personali.
- **Rilevamento** **malware**
  Monitoraggio costante delle vulnerabilità del sito e immediata risoluzione.

Il sito web è accessibile per la gestione dei contenuti previa creazione di credenziali fornite dall'amministratore del sito.

Misure sulla protezione dei dati adottata

Le password vengono criptate sul Database con l'algoritmo di hashing **bcrypt**. Bcrypt è una funzione adattiva: col tempo, il conteggio dell'iterazione può essere aumentato per renderla più lenta, in modo da essere resistente ad attacchi di forza bruta anche con capacità computazionale crescente. Vengono utilizzati dei cookies tecnici per la attività di monitoraggio del sito web, per la generazione di report relativi agli accessi effettuati, al numero di pagine visitate dagli utenti. I cookies utilizzati sono quelli di Google Analytics con anonimizzazione degli indirizzi IP dei visitatori per impedire a Google di eseguire attività di profilazione.

Nessun dato relativo agli utenti viene trattato o storicizzato per alcuna finalità. L'informativa sulla privacy è disponibile su apposita pagina del sito web al seguente indirizzo https://www.comune.ittiri.ss.it/pg/privacy-policy/21

Sito Istituzionale Visit Ittiri.com

Il sito web è ospitato su hosting server dedicato dislocato nei data center di Seflow snc presso Settimo Milanese e presidiata 24 ore su 24 da personale specializzato. E' garantito l'accesso remoto tramite adozione diversi protocolli di comunicazione e l'utilizzo di specifiche credenziali di amministratore.
Il server è protetto da intrusioni esterne tramite adozione di specifiche regole sul firewall del sistema operativo, che ne garantiscono l'accesso solo al personale della Consulmedia da una rete predefinita. Il sito web è accessibile per la gestione dei contenuti previa creazione di credenziali fornite dall'amministratore del sistema. L'utenza di amministratore per la creazione di nuovi utenti è in gestione alla Consulmedia, che rilascia le nuove utenze attraverso specifica richiesta scritta.

Eventuali misure di sicurezza da adottare
Installazione di un certificato ssl per la comunicazione tramite protocollo sicuro https. Eventualmente siamo disponibili a fornire tale misura di sicurezza sotto preventivo per vostra valutazione dei costi.

Misure sulla protezione dei dati adottata
Vengono utilizzati dei cookies tecnici per la attività di monitoraggio del sito web, per la generazione di report relativi agli accessi effettuati, al numero di pagine visitate dagli utenti
I cookies utilizzati sono quelli di Google Analytics con anonimizzazione degli indirizzi IP dei visitatori per impedire a Google di eseguire attività di profilazione.
Nessun dato relativo agli utenti viene trattato o storicizzato per alcuna finalità.
E' implementato un meccanismo di accettazione o rifiuto dei cookies attraverso una nota informativa mostrata in fase di apertura del sito web, dove l'utente può decidere o meno se prestare il consenso all'utilizzo dei cookies. La non accettazione dell'informativa comporta la non accettazione all'utilizzo dei cookies e quindi al tracciamento delle attività effettuate dall'utente. Successivamente all'accettazione è possibile rimuovere i cookies con modalità che variano in base al browser utilizzato per la navigazione del sito web.
L'informativa sulla privacy è disponibile su apposita pagina del sito web al seguente indirizzo
http://www.visitittiri.com/logudorogoceanogal/opencms/it/utilita/privacy/