

AUDIT SISTEMA INFORMATIVO

rELAZIONE SISTEMA INFORMATIVO ACETIFICIO VARVELLO

sISTEMI TRE S.R.L.

2019

Il presente documento ha come obiettivo quello di descrivere gli aspetti più rilevanti del sistema informativo del cliente.

Gli ambiti che verranno descritti e analizzati sono i seguenti:

1. **Infrastruttura fisica e rete wireless**
   * Struttura logica network
   * Struttura fisica network
   * Elenco VLAN e Network
   * Elenco apparati network
2. **Connettività Internet**
3. **Firewall e Sicurezza Perimetrale**
4. **Infrastruttura Server e locali tecnici**
   * Infrastruttura Vmware
   * Infrastruttura Server Fisici
   * Infrastruttura Active Directory, DNS e DHCP
   * Licenze Software in uso
5. **Infrastruttura di messaging**
6. **Infrastruttura Backup e DR**
7. **Telefonia**
8. **Analisi dei rischi**

# **INFRASTRUTTURA FISICA E RETE WIRELESS**

Per quanto riguarda l’infrastruttura fisica la rete di accesso cablata in rame è in categoria 5.

I vari armadi sono situati in locali dedicati e di facile accesso per le manutenzioni tecniche.

**STRUTTURA FISICA RETE**



Firewall Sophos XG115

Switch Armadio Rack sala server 1° Piano – Unifi Switch 48 porte.

# 

Internet

# 

Switch Armadio Laboratorio – Unifi Switch 48 porte poe.

Switch Armadio Uffici 1° Piano – Unifi Switch 48 porte poe.

# 

Switch Armadio Magazzino Produzione – Unifi Switch 48 porte poe.

Switch Armadio Magazzino Automatizzato – Unifi Switch 48 porte poe.

Sono presenti anche n° 6 access point Unifi AP-AC-Pro per collegamento terminali gestione magazzino, dispositivi mobili e smartphone.

# **ELENCO VLAN**

Di seguito sono riportate le VLAN rilevate

|  |  |  |  |
| --- | --- | --- | --- |
| Nome | VLAN ID | Network | Note |
| NET LAN | 1 | 192.168.1.0/24 |  |
| NET GUEST | 2 | 192.168.200.0/24 | Rete Wi-Fi Ospiti |
| NET VOCE | 200 | 10.200.1.0/24 |  |

# **ELENCO APPARATI NETWORK**

Di seguito è riportato l’elenco degli apparati attivi dedicati al network (switch)

|  |  |  |  |
| --- | --- | --- | --- |
| Modello | Indirizzo IP | Location | Note |
| SWITCH01-LOCALE SERVER | 192.168.1.241 | Sala Server – CED | Unifi Switch 48 porte |
| SWITCH02-LOCALE UFFICI | 192.168.1.242 | Armadio Uff. | Unifi Switch 48 porte poe |
| SWITCH03-LOCALE MAG AUT. | 192.168.1.243 | Armadio Mag. Aut. | Unifi Switch 48 porte poe |
| SWITCH04-LOCALE LAB. | 192.168.1.244 | Armadio Uff. Lab. | Unifi Switch 48 porte poe |
| SWITCH05-LOCALE MAG. PROD. | 192.168.1.125 | Armadio Mag. Prod. | Unifi Switch 48 porte poe |

# **ACCESSO INTERNET**

Le connettività Internet sono fornite dall’operatore ISP BBBELL tramite una connessione in Ponte Radio.

# **SICUREZZA PERIMETRALE**

La sicurezza perimetrale viene gestita attraverso la combinazione delle policy applicate sul firewall Sophos XG115 presente nell’armadio locale server.

# **INFRASTRUTTURA SERVER E LOCALI TECNICI**

Il datacenter risiede in un locale dedicato senza controlli accesso. L’armadio rack è alimentato e interamente alimentato e protetto da un gruppo di continuità dedicato. Il locale è ben condizionato.

# **INFRASTRUTTURA:**

Nell’armadio rack del locale server è presente quanto segue:



N°1 SERVER Lenovo SR650

HOST VMWare per la gestione di server virtuali Microsoft Windows Server:

|  |  |
| --- | --- |
| 192.168.1.232 | SRV-DC01 (*DOMAIN CONTROLLER*) |
| 192.168.1.233 | SRV-GEST01 (*ENOLOGIA*) |
| 192.168.1.234 | SRV-TS01 (*RDP PER SEDI REMOTE*) |
| 192.168.1.238 | SRV-SCADA |
| 192.168.1.239 | SRV-LOGISTICA (*GESTIONE MAGAZZINO*) |
| 192.168.1.200 | VARVELLO-SERVER (*FILE SYSTEM AZIENDALE*) |



N°1 SERVER LENOVO SR650

Server fisico con Windows Server per la gestione magazzino automatizzato.

|  |  |
| --- | --- |
| 192.168.1.237 | SRV-SPAGGIARI01 |

N° 2 NAS QNAP per la gestione dei backup server fisici e virtuali tramite software di backup Veeam Backup & Replication installato su server SRV-DC01 attualmente situati nell’armadio rack sala server.



|  |  |
| --- | --- |
| 192.168.1.204 | NAS02 |
| 192.168.1.235 | NAS01 |

# **SEDE REMOTA (MODENA):**

L’infrastruttura comprende un armadi rack con i seguenti apparati:

* + - * Switch 10/100
      * Firewall Sophos XG 105
      * DVR per gestione video sorveglianza
      * Apparati connettività internet – ADSL + Ponte Radio

Sono presenti n°3 postazioni che si collegano tramite protocollo RDP per accesso gestionale Enologia.

Il collegamento avviene tramite VPN Site-to-Site instaurato tra i due firewall Sophos.

# **RETI WIRELESS:**

Come già descritto la copertura Wi-Fi è gestita da apparati Unifi con portale di manutenzione in cloud. Attualmente sono presenti due reti:

* + - * VARVELLO-WIFI (ad uso aziendale per dispositivi mobili)
      * VARVELLO-GUEST (per operatori esterni, solo accesso internet e blocco verso rete aziendale)
      * VARVELLO-TERM (ad uso aziendale per terminali magazzino)

# **INFRASTRUTTURA ACTIVE DIRECTORY, DNS E DHCP**

L’azienda dispone di una propria infrastruttura Active Directory per la gestione degli utenti, policy aziendali.

I servizi DNS e DHCP sono delegati alla realtà aziendale e dispongono di una gestione indipendente.

I livelli di funzionalità delle foreste e dei domini AD sono Windows 2016.

# **LICENZE SOFTWARE**

I Sistemi Operativi sono in genere correttamente licenzianti, si rileva la presenza di versioni queste Windows:

* + - * Windows Server 2016
      * Windows 7 Pro
      * Windows 10 Pro
      * Windows Server 2008 R2

I software aziendali sono in genere correttamente licenziati, le versioni di office presenti sulle varie postazioni variano da una versione minima di Office 2010 a Office 2013.

Tutte le postazioni di lavoro sono dotate di antivirus Sophos distribuito e gestito tramite portale in cloud.

# **INFRASTRUTTURA DI MESSAGING**

Il servizio di messaging (mail) si basa su una soluzione cloud Gmail.

# **INFRASTRUTTURA BACKUP E DR**

Il backup per l’ambiente Vmware è schedulato giornalmente su due NAS con il Software Veeam Backup & Replication. Sono presenti anche politiche di backup delle singole postazioni tramite il medesimo software.

# **TELEFONIA**

La telefonia è gestita da un centralino VoIP (gestito dal provider di connettività BBBELL) , suddivisi tra cordless e fissi. Il sistema è gestito direttamente dal fornitore senza possibilità di assistenza remota. È presente un sistema DECT interfacciato ai cordless.

# **ANALISI DEI RISCHI**

A seguito dell’analisi svolta riportiamo sotto la tabella riassuntiva sull’analisi dei rischi aziendali, in una scala di punteggio da 1 a 10.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **LIVELLO DI SERVIZIO** | **ADEGUATEZZA** | **CONFIGURAZIONE E UTILIZZO** | **AFFIDABILITA’** | **MEDIA LIVELLO DI SERVIZIO** |
| **Infrastruttura LAN** | **9** | **9** | **9** | **9** |
| **Connettività Internet** | **8** | **8** | **8** | **8** |
| **Sicurezza Perimetrale** | **9** | **9** | **8** | **8,66** |
| **Infrastruttura Server** | **9** | **9** | **8** | **8,66** |
| **Infrastruttura di Messaging** | **9** | **9** | **9** | **9** |
| **Infrastruttura Backup e DR** | **8** | **8** | **8** | **8** |
| **Telefonia** | **7** | **7** | **8** | **7,33** |

\*\* Adeguatezza: indica lo stato d’idoneità della soluzione in conformità al ruolo svolto

\*\* Configurazione: indica quanto la soluzione è correttamente configurata in conformità al ruolo svolto

\*\* Affidabilità: indica la criticità in caso di guasto o disservizio