|  |  |  |  |
| --- | --- | --- | --- |
| **SISTEMA INFORMATICO**  **DELLA PRO LOCO “\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_”** | | | |
|  | **MODELLO** | **CARATTERISTICHE** | **NOTE** |
| **SERVER FISICO** |  |  |  |
| **SERVER VIRTUALE** |  |  |  |
| **NAS** |  |  |  |
| **SISTEMA BACK UP** |  |  |  |
| **FIREWALL** |  |  |  |
| **ROUTER** |  |  |  |
| **ACCESS POINT** |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **modello** | **chi è il proprietario** | **chi lo usa** | **antivirus** | **back up e altre informazioni** |
| **PC 1** |  |  |  |  |  |
| **PC 2** |  |  |  |  |  |
| **PC 3** |  |  |  |  |  |
| **Portatile 1** |  |  |  |  |  |
| **Portatile 2** |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **MISURE DI SICUREZZA INFORMATICHE** | | | | |
| **MISURA** | **SI** | **NO** | **STATO ATTUALE** | **NOTE – MISURE DA ADOTTARE** |
| **SISTEMA DI IDENTIFICAZIONE** |  |  | *Tutte le persone che trattano dati con strumenti informatici sono identificate con apposita credenziale (nome utente)* |  |
| **SISTEMA DI AUTENTICAZIONE** |  |  | *Tutti gli accessi ai dati sono soggetti a USERNAME e PASSWORD per ogni operatore* |  |
|  |  | *Tutti gli accessi alle caselle-mail sono soggetti a password per ogni utente con cambio periodico* |  |
|  |  | *In caso di accessi da nuovi “device” si obbliga ad autorizzazione che permette l’accesso ai dati (altrimenti vietato)* |  |
| **SISTEMA DI AUTORIZZAZIONE** |  |  | *Per ogni incaricato sono definiti specifici profili di autorizzazione determinati a livello di sistema di gestione e permessi esclusivamente con password* |  |
| **CARTELLE INFORMATICHE CON DATI PARTICOLARI CIFRATURA E/O PROTEZIONE DEI DATI** |  |  | *Definite specifiche cartelle con accesso limitato contenente dati particolari*  *Definite specifiche cartelle con accesso limitato contenente dati sanitari o giudiziari (ove necessario)*  *cartelle criptate per conservare dati sensibili o ultrasensibili* |  |
| **PROCEDURA MODIFICA CREDENZIALI** |  |  |  |  |
| **PROCEDURA**  **PER BACK-UP** |  |  |  |  |
| **DISASTER RECOVERY** |  |  |  |  |
| **MODALITA’ DI DISMISSIONE DI PC E STAMPANTI** |  |  |  |  |
| **LIMITAZIONE SITI PERICOLOSI** |  |  |  |  |
| **LIMITAZIONE TRAFFICO DATI DA SISTEMI INFORMATICI** |  |  |  |  |
| **IDENTIFICATO E NOMINATO AMMINISTRATORE DI SISTEMA** |  |  |  |  |
| **PROCEDURA DI CANCELLAZIONE DEI DATI** |  |  |  |  |
| **DATI CHE RISIEDONO SUL SITO WEB** |  |  | *I dati inseriti nelle FORM sono conservati per un massimo di \_\_\_\_\_ giorni dopo la compilazione e poi vengono automaticamente cancellati. In ogni caso i dati sono passati all’interno dell’organizzazione e quindi quelli sul sito solo considerati solo una copia temporanea.* |  |
| **SISTEMA DI RILEVAZIONE E BLOCCO DELLE CONNESSIONI E DELLE INTRUSIONI DA ESTERNO** |  |  |  |  |
| **SISTEMA DI CONTROLLO DEGLI AGGIORNAMENTI DEI SISTEMI OPERATIVI** |  |  |  |  |
| **SISTEMA DI CONTROLLO DEGLI AGGIORNAMENTI DEGLI ANTIVIRUS E FIREWALL** |  |  |  |  |
| **CONTROLLO ACCESSI WI-FI E REGOLE PER L’USO** |  |  |  |  |
| **SISTEMI DI MANTENIMENTO DELLA FUNZIONALITÀ IN CASO DI ASSENZA IMPROVVISA DI ENERGIA ELETTRICA** |  |  | *È presente un gruppo di continuità per il server e i seguenti PC* |  |
| **CLIMATIZZAZIONE DEI LOCALI DEI SERVER** |  |  |  |  |
| **SISTEMA ANTI INTRUSIONE** |  |  | *In orario di lavoro gli ingressi ai locali sono presidiati da personale*  *È attivo un sistema di videosorveglianza* |  |
| **SITI E WEB CON**  **SISTEMI HTTPS** |  |  |  |  |
| **REGISTRAZIONE DEGLI ACCESSI** |  |  |  |  |
| **SISTEMA DI LOG-OUT** |  |  |  |  |
| **SISTEMI DI RILEVAZIONE DELLE EMERGENZE** |  |  | *Incendio*  *Allagamento*  *Onde sonore*  *campi elettromagnetici* |  |
| **ULTERIORI SISTEMI DI PROTEZIONE** |  |  |  |  |