# Allevamento ittico

## Jacopo Mattia Marconi

### Indice

1. ANALISI DEL PROBLEMA:

Il contesto:

* Studiamo il contesto di una società che gestisce vasche a temperatura controllata per l’allevamento di pesci tropicali. L’allevamento consiste in una serie di vasche totalmente autosufficienti per fornire l’illuminazione e l’alimentazione necessarie alle diverse specie presenti. Ogni vasca è dotata di una serie di sensori per impostare, tramite degli attuatori, le condizioni ottimali per la specie di pesce contenuta (es. quantità di nutrienti, ciclo di illuminazione, temperatura dell’acqua, ecc…). Le vasche, quando sono in sede, sono collegate a un sistema centrale attraverso la rete aziendale a cui trasmettono tutti i parametri rilevati e da cui ricevono le impostazioni di funzionamento. Nel database del sistema centrale sono memorizzate le informazioni specifiche di configurazione standard dell’azienda e le necessità delle diverse specie di pesci da utilizzare per l’impostazione delle vasche. La società rende disponibile un servizio di noleggio per utenti esterni (ad esempio fiere che inseriscono le vasche come elemento di arredamento temporaneo); in tal caso le vasche per poter funzionare devono potersi collegare al sistema di gestione centrale. Gli utenti possono collegarsi ad un’applicazione per acquistare il servizio e per verificare lo stato della propria vasca. Settimanalmente la società deve generare la bolletta di pagamento per i propri clienti, a tal proposito è necessario conteggiare il consumo effettivo di ogni vasca noleggiata (costo fisso orario, nutrienti ed energia consumati).

Informazioni aggiuntive:

* Ipotizziamo che la società sia composta da una singola sede centrale comprensiva di vertice strategico, linea intermedia e nucleo operativo con ampia zona di esposizione per le vasche. Quest’ultime possono variare in peso, lunghezza, larghezza e profondità, conseguentemente a ciò, ogni vasca possiede un costo fisso qualora venga noleggiata. L’azienda possiede diversi modelli di vasche e per ogni modello ci possono essere una o più vasche prodotte. Le vasche dispongono di un’interfaccia di rete ethernet, con connettore standard RJ-45, e di un’interfaccia di rete wireless, con standard Wi-Fi 4 (IEEE 802.11n) con velocità 72-600 Mbit/s e frequenze di 2.4 o 5 GHz. Ogni singola vasca è dotata di uno schermo touch resistivo, per facilitarne l’uso del personale tramite guanti protettivi (necessari sul luogo di lavoro). Tramite lo schermo touch è possibile visualizzare informazioni primarie come temperatura, livello di ossigeno, livello dell’acqua e tipologia di pesci contenuti. Dal medesimo schermo è possibile accendere e spegnere le luci interne ed esterne della vasca (funzionalità pensata a fini dimostrativi). Le vasche situate all’interno dell’azienda possono essere collegate indipendentemente tramite rete cablata o wireless al sistema informativo centrale composto da un database server MySQL interno (non raggiungibile dalla rete internet) raggiungibile, invece, da un server web (posto in DMZ). I clienti possono accedere all’area riservata in seguito ad una autenticazione con mail e password personali attraverso il sito web aziendale. Le vasche noleggiate dai clienti, e ovviamente poste all’esterno dell’azienda, possono essere a loro volta collegate tramite rete cablata o wireless, a seconda delle esigenze, e comunicano al sistema centrale dell’azienda tramite VPN Site-to-site con protocollo di tunneling Ipsec. I clienti che usufruiscono del servizio di noleggio (unico servizio proposto dall’azienda, per garantire supporto e qualità) devono necessariamente possedere una partita iva, senza la quale non è possibile noleggiare le vasche. L’azienda dispone di un servizio di supporto telefonico di pronto intervento a tempo pieno.

Il sito web aziendale dispone di:

* una sezione composta da informazioni aziendali (storia, inizi, numeri, personale, politica d’impresa, ecc…);
* una sezione di vendita per le aziende del servizio di noleggio delle vasche con un catalogo delle vasche disponibili al noleggio e le relative informazioni (misure, costo, materiali utilizzati, ecc…);
* una sezione riservata, con accesso tramite mail e password personali, con differenti autorizzazioni in base al ruolo di ciascuno per l’azienda (personale interno o clienti);

Quando un nuovo utente si registra tra i campi richiesti ci saranno mail e password, quest’utlime saranno le credenziali di accesso all’area riservata. Il personale si dovrà registrare con la mail aziendale.

L’utente “cliente”:

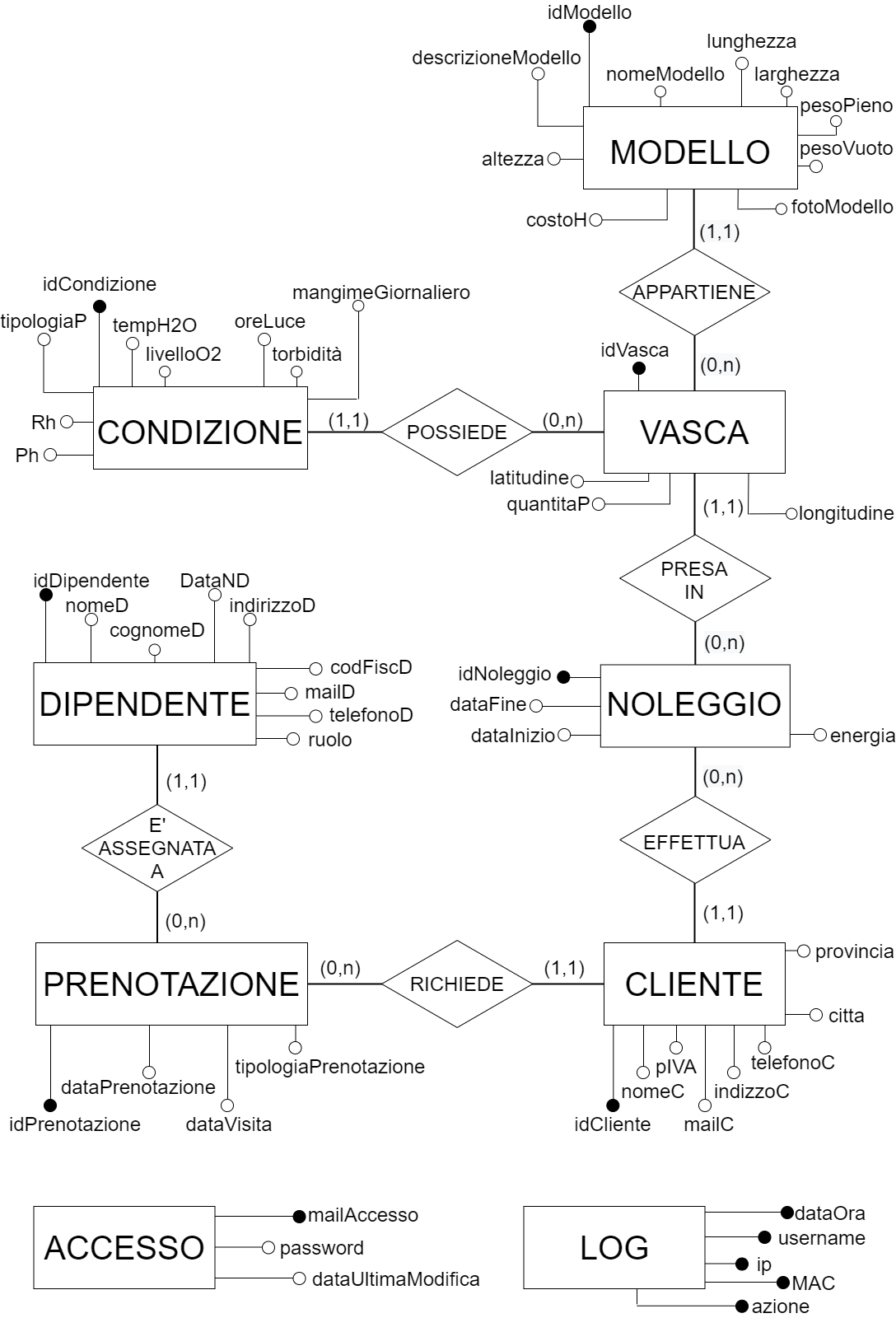
* Dopo aver eseguito l’accesso tramite autenticazione con mail e password personali, il singolo cliente potrà visualizzare lo stato completo della sua vasca e il costo fisso orario, nonché il costo totale dall’inizio del noleggio; è possibile visualizzare, inoltre, lo storico relativo ai noleggi delle vasche dell’utente stesso. In ogni momento, l’utente “cliente” è in grado di visualizzare lo storico dei dati relativi ad ogni singola vasca posseduta da lui stesso.

L’utente “personale”:

* Il personale interno dell’azienda, una volta effettuato l’accesso all’area riservata, è in grado di controllare lo stato di ciascuna vasca, interna all’azienda o noleggiata da un cliente, per monitorare lo stato di ciascuna e intervenire prontamente in caso di necessità.

Il sito web è scritto prevalentemente in PHP, per la facile integrazione con i servizi offerti da MySQL.

Oltre al sito web e all’area riservata al suo interno accessibile da ogni utente sarà necessario implementare un servizio di gestione interno all’azienda. Questo ulteriore servizio sarà sempre implementato tramite una web application in locale e sarà accessibile solamente ai dipendenti autorizzati. La web application in questione avrà il compito di monitorare e permettere all’utente di aggiornare i dati presenti nel database aziendale e di assegnare il personale alle singole prenotazioni online effettuate dai clienti bisognosi di assistenza tecnica o di un sopraluogo da parte di un dipendente (tecnico) dell’azienda stessa.



NOTE:

* Condizione: ogni condizione descrive i valori ideali dell’habitat riferiti alla tipologia di pesce.

L’attributo *mangimeGiornaliero* rappresenta i grammi di cibo che giornalmente ogni singolo pesce deve assumere.

* Modello: il costo orario di ogni singola modello di vasca dipende dalle misure del modello stesso.

Gli attributi *nomeModello* e *fotoModello* hanno uno scopo puramente espositivo, utilizzati nel sito web.

* Vasca: ogni vasca è dotata di GPS per motivi di sicurezza.

L’attributo *quantitaP*, riferito alla quanità dei pesci presenti, può essere null se la vasca non è in utilizzo o non è “abitata”.

* Noleggio: al momento del contratto di noleggio viene indicata la durata del noleggio stesso, per questo motivo l’attributo *dataFIne* non è opzionale.

L’attributo *energia* contiene il dato dell’energia consumata dall’inizio del noleggio, aggiornata giornalmente.

* Cliente: l’azienda permette il noleggio delle vasche solamente ai clienti dotati di partita IVA.
* Prenotazione: un cliente può richiedere una prenotazione online descrivendo solamente la tipologia di intervento richiesto. L’attributo *dataPrenotazione* si riferisce alla data nella quale il cliente richiede la prenotazione. L’attributo dataVisita è opzionale, viene aggiunto dal personale autorizzato interno dopo aver visionato le disponibilità dell’azienda.
* Dipendente: in base al ruolo ogni dipendente potrà, o meno, accedere al servizio di gestione interno dell’azienda o di essere disponibile ad essere mandato in assistenza esterna presso un cliente.
* Accesso: l’entità *Accesso* si riferisce agli accessi all’area riservata del sito web. Ogni accesso è diversificato grazie alla mail, che definisce univocamente l’entità stessa.

L’attributo *dataUltimaModifica* è necessario per permettere all’utente di cambiare password di accesso ogni 3 mesi.

* Log: l’entità Log viene utilizzata per tenere traccia di ogni azione svolta all’interno dell’area riservata. Ogni record memorizzato viene cancellato dopo 6 mesi.

L’attributo *MAC* è opzionale poichè è possibile tenerne traccia solo se l’ip è locale.

Documentazione delle ENTITA’:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NOME | DESCRIZIONE | ATTRIBUTI | OPZ. ATTR. | TIPO | DOMINIO |
| Condizione | L’entità *Condizione* contiene le informazioni sulle diverse condizioni che ogni vasca possiede a seconda della tipologia di pesce. | **idCondizione PK**  tipologiaP  tempH2O  livelloO2  oreLuce  torbidità  mangimeGiornaliero  Rh  Ph | No  No  No  No  No  No  No  No  No | Int  Varchar 20  Int  Float  Int  Int  Int  Int  Int  Int | >0  >=0  >=0  >=0  >0  >200  >0 |
| Modello | L’entità *Modello* contiene le informazioni proprie di un modello. | **idModello PK**  nomeModello  fotoModello  costoH  lunghezza  larghezza  altezza  pesoVuoto  pesoPieno  descrizioneModello | No  No  Si  No  No  No  No  No  No  No | Int  Varchar 20  Blob  Float  Float  Float  Float  Int  Int  Varchar 300 | >0  >0 && <600 >0 && <200  >0 && <250  >0  >pesoVuoto |
| Vasca | L’entità *Vasca* contiene le informazioni proprie di una vasca. | **idVasca PK**  quantitaPesci  latitudine  longitudine | No  Si  No  No | Int  Int  Double  Double | >=0 |
| Noleggio | L’entità *Noleggio* contiene le informazioni relative ai noleggi delle vasche effettuati dai clienti | **idNoleggio PK**  dataInizio  dataFine  energia | No  No  No  No | Int  Date  Date  Float | >dataInizio  >=0 |
| Cliente | L’entità *Cliente* contiene le informazioni relative ad ogni singolo cliente | **idCliente PK**  nomeC  pIVA  mailC  indirizzoC  telefonoC  citta  provincia | No  No  No  No  No  No  No  No | Int  Varchar 20  Char (11)  Varchar 20  Varchar 20  Char (10) |  |
| Prenotazione | L’entità *Prenotazione* contiene le informazioni relative ad ogni prenotazione di visita di un tecnico da parte di un cliente. | **idPrenotazione PK**  dataPrenotazione  dataVisita  tipologiaPrenotazione | No  No  Si  No | Int  Date  Date  Varchar 30 | {sopraluogo, assistenza tecnica, collaborazione, assistenza all’acquisto} |
| Dipendente | L’entità *Dipendente* si riferisce alle informazioni utili di ogni dipendente dell’azienda | **idDipendente PK**  nomeD  cognomeD  dataND  indirizzoD  codfiscD  mailD  telefonoD  ruolo | No  No  No  No  No  No  No  No  No | Int  Varchar 20  Varchar 20  Date  Varchar 20  Char 16  Varchar 20  Char 10  Varchar 20 | {tecnico, amministrativo, personale} |
| Accesso | L’entità *Accesso* contiene i dati relativi all’accesso all’area riservata del sito web aziendale | **mailAccesso PK**  dataUltimaModifica  password | No  No  No | Varchar 20  date  Varchar 20 | >8 caratteri (>1 maiuscola, >1 carattere speciale, >1 numero, no sequenze di alcun tipo) |
| Log | L’entità *Log* contiene i dati di ogni singola azione svolta da un utente all’interno dell’area riservata del sito web aziendale | **dataOra PK**  **username PK**  **ip PK**  **MAC PK**  **Azione PK** | No  No  No  Si  No | DateTime  Varchar 20  Varchar 15  Varchar 17  Varchar 20 |  |

Documentazione delle ASSOCIAZIONI:

|  |  |  |  |
| --- | --- | --- | --- |
| NOME | DESCRIZIONE | ENTITA’ COINVOLTE | ATTRIBUTI |
| possiede | L’associazione *possiede* descrive il legame tra le vasche e le relative condizioni | Condizione  Vasca |  |
| appartiene | L’associazione *appartiene* descrive il legame tra i modelli e le vasche prodotte | Modello  Vasca |  |
| presa in | L’associazione *presa in* descrive il legame tra le vasche e i relativi noleggi | Vasca  Noleggio |  |
| effettua | L’associazione *effettua* descrive il legame tra i noleggi e i clienti | Noleggio  Cliente |  |
| richiede | L’associazione *richiede* descrive il legame tra i clienti e le prenotazioni effettuate | Cliente  Prenotazione |  |
| è assegnata a | L’associazione *è assegnata a* descrive il legame tra le prenotazioni e i dipendenti a cui sono affidate le prenotazioni | Prenotazione  Dipendente |  |

CREATE DATABASE vascheittiche;

CREATE TABLE accessi (

mailAccesso varchar(40) NOT NULL,

dataUltimaModifica date NOT NULL,

password varchar(20) NOT NULL,

PRIMARY KEY (mailAccesso));

CREATE TABLE clienti (

idCliente int(5) NOT NULL,

nomeCliente varchar(30) NOT NULL,

pIVA char(11) NOT NULL,

mailCliente varchar(40) NOT NULL,

indirizzoCliente varchar(30) NOT NULL,

telefonoCliente char(10) NOT NULL,

citta varchar(30) NOT NULL,

provincia varchar(30) NOT NULL,

PRIMARY KEY (idCliente));

CREATE TABLE condizioni (

idCondizione int(5) NOT NULL,

tipologiaP varchar(30) NOT NULL,

tempH2O int(11) NOT NULL,

livelloO2 float NOT NULL,

oreLuce int(11) NOT NULL,

torbidita int(11) NOT NULL,

mangimeGiornaliero int(11) NOT NULL,

Rh int(11) NOT NULL,

Ph int(11) NOT NULL,

PRIMARY KEY (idCondizione));

CREATE TABLE dipendenti (

idDipendente int(5) NOT NULL,

nomeDipendente varchar(30) NOT NULL,

cognomeDipendente varchar(30) NOT NULL,

dataNDipendente date NOT NULL,

indirizzoDipendente varchar(30) NOT NULL,

codFiscDipendente char(16) NOT NULL,

mailDipendente varchar(40) NOT NULL,

telefonoDipendente char(10) NOT NULL,

ruoloDipendente varchar(20) NOT NULL,

PRIMARY KEY (idDipendente));

CREATE TABLE log (

dataOra datetime NOT NULL,

username varchar(30) NOT NULL,

ip varchar(15) NOT NULL,

MAC varchar(17) DEFAULT NULL,

azione varchar(30) NOT NULL,

PRIMARY KEY (dataOra, username, ip, MAC, azione));

CREATE TABLE noleggi (

idNoleggio int(5) NOT NULL,

dataInizio date NOT NULL,

dataFine date NOT NULL,

energia float NOT NULL,

idCliente int(5) NOT NULL,

idVasca int(5) NOT NULL,

PRIMARY KEY (idNoleggio),

FOREIGN KEY (idCliente) REFERENCES clienti (idCliente),

FOREIGN KEY (idVasca) REFERENCES vasche (idVasca));

CREATE TABLE prenotazioni (

idPrenotazione int(5) NOT NULL,

dataPrenotazione date NOT NULL,

dataVisita date NOT NULL,

tipologiaPrenotazione varchar(30) NOT NULL,

idCliente int(5) NOT NULL,

idDipendente int(5) DEFAULT NULL,

PRIMARY KEY (idPrenotazione),

FOREIGN KEY (idCliente) REFERENCES clienti (idCliente),

FOREIGN KEY (idDipendente) REFERENCES dipendenti (idDipendente));

CREATE TABLE modelli (

idModello int(5) NOT NULL,

nomeModello varchar(30) NOT NULL,

fotoModello longblob DEFAULT NULL,

costoH float NOT NULL,

lunghezza float NOT NULL,

larghezza float NOT NULL,

altezza float NOT NULL,

pesoVuoto int(11) NOT NULL,

pesoPieno int(11) NOT NULL,

descrizioneModello varchar(100) NOT NULL

PRIMARY KEY (idModello));

CREATE TABLE vasche (

idVasca int(5) NOT NULL,

quantitaPesci int(11) DEFAULT NULL,

latitudine varchar(10) NOT NULL,

longitudine varchar(10) NOT NULL,

idCondizione int(5) NOT NULL,

idModello int(5) NOT NULL,

PRIMARY KEY (idVasca),

FOREIGN KEY (idCondizione) REFERENCES condizioni (idCondizione),

FOREIGN KEY (idModello) REFERENCES modelli (idModello));

Condizioni(idCondizione, tempH2O, livelloO2, oreLuce, mangimeGiornaliero, torbidita, Rh, Ph, tipologiaP)

Modelli(idModello, costoH, lunghezza, larghezza, altezza, pesoVuoto, pesoPieno, fotoModello, descrizioneModello, nomeModello)

Vasche(idVasca, quantitaP, latitudine, longitudine, idCondizione, idModello)

Noleggi(idNoleggio, dataInizio, dataFine, energia, idVasca, idCliente)

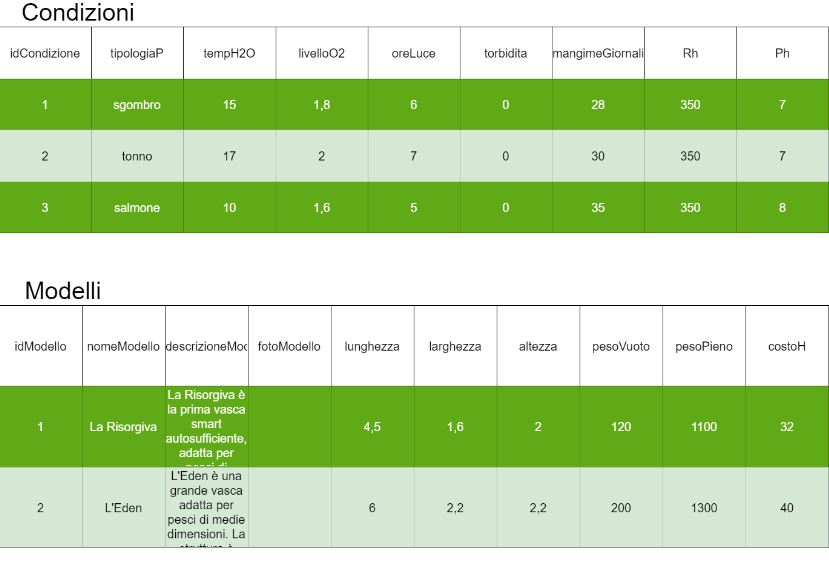
Clienti(idCliente, nomeCliente, pIVA, mailCliente, indirizzoCliente, telefonoCliente, citta, provincia)

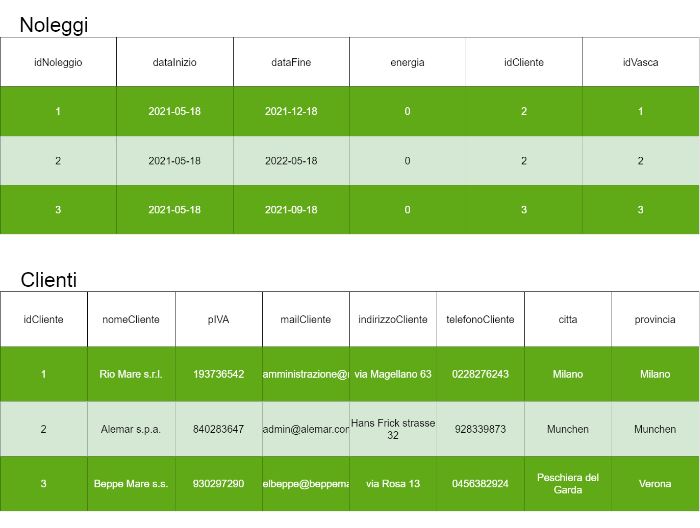
Prenotazioni(idPrenotazione, dataPrenotazione, dataVisita, tipologiaPrenotazione, idCliente, idDipendente)

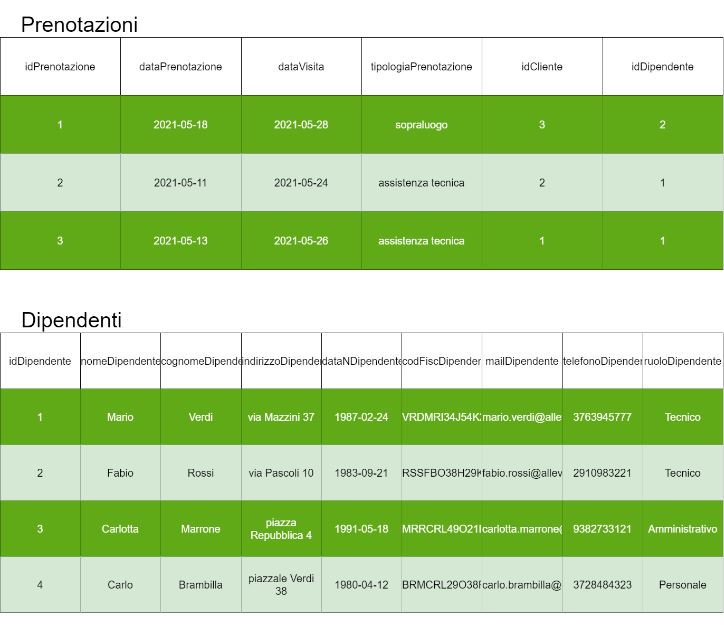
Dipendenti(idDipendente, nomeDipendente, cognomeDipendente, dataNDipendente, indirizzoDipendente, codFiscDipendente, mailDipendente, telefonoDipendente, ruolo)

Accessi(mailAccesso, password, dataUltimaModifica)

Log(dataOra, username, ip, MAC, azione)









Esempio query significative:

* Trovare i dipendenti (solo tecnici) con meno impegni programmati. Il risultato di questa query sarà utile al personale interno autorizzato per poter assegnare equamente gli impegni tra i tecnici presenti:

create view impegniDipendenti as SELECT d.idDipendente, COUNT(\*) AS impegniDipendente from prenotazioni p right JOIN dipendenti d ON p.idDipendente=d.idDipendente GROUP BY (d.idDipendente);

SELECT d.idDipendente, d.nomeDipendente, d.cognomeDipendente, i.impegniDipendente from impegniDipendenti i JOIN dipendenti d ON d.idDipendente=i.idDipendente where i.impegniDipendente=(select min(impegniDipendente) from impegniDipendenti) AND d.ruoloDipendente="Tecnico";

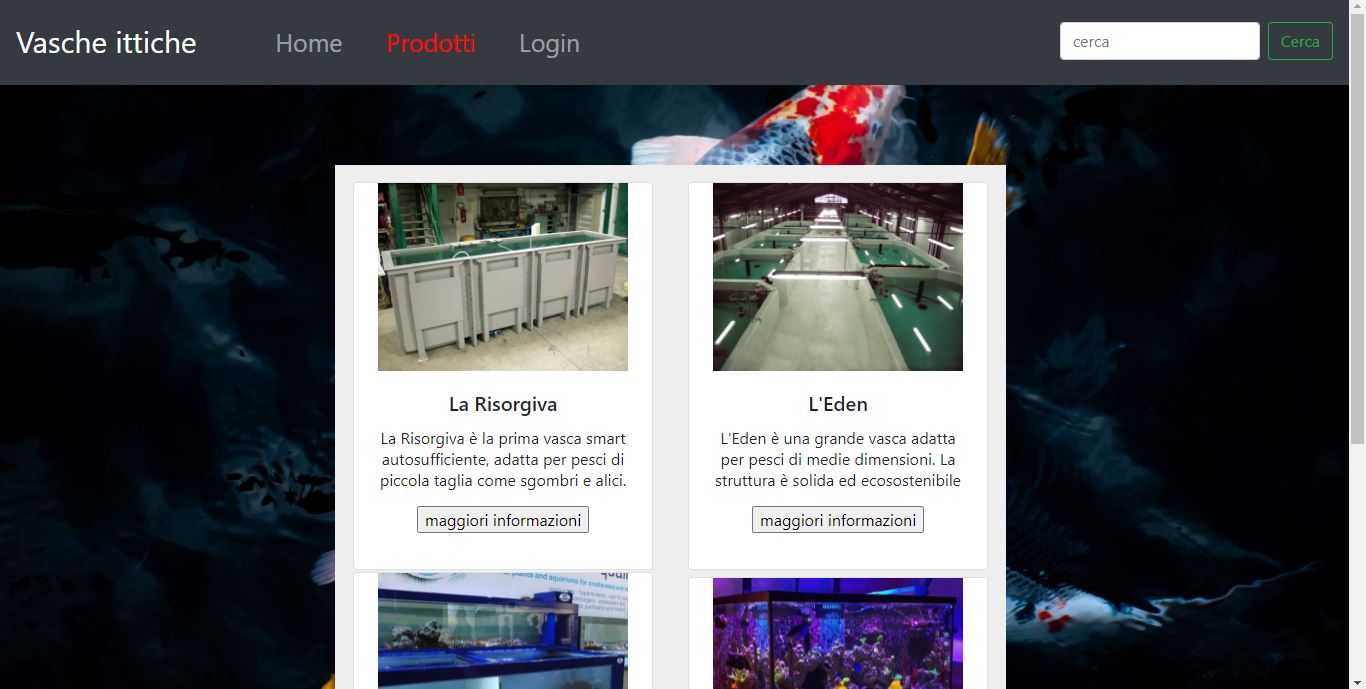
|  |  |  |  |
| --- | --- | --- | --- |
| idDipendente | nomeDipendente | cognomeDipendente | impegniDipendente |
| 2 | Fabio | Rossi | 1 |

* Trovare il modello di vasca più noleggiato:

create view noleggiModelli as SELECT m.idModello, COUNT(\*) AS noleggiModello FROM noleggi n join vasche v ON v.idVasca=n.idVasca join modelli m ON m.idModello=v.idModello group BY (m.idModello);

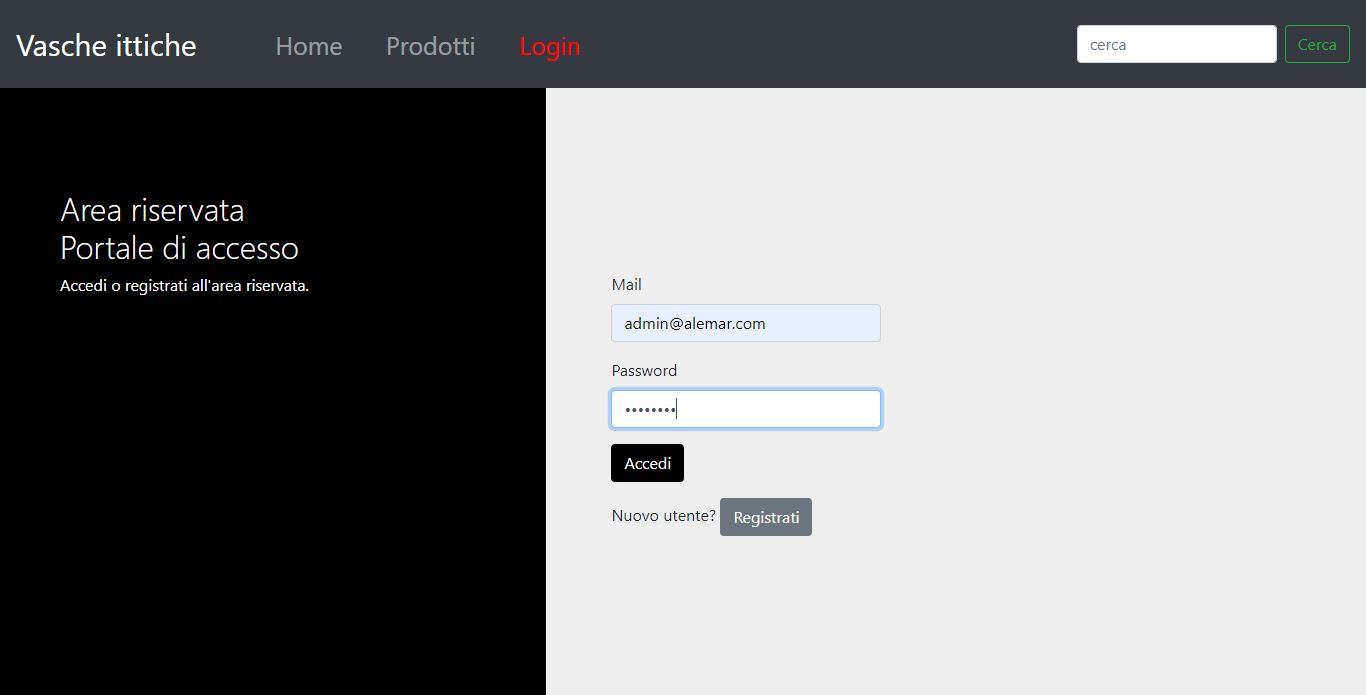
SELECT nm.idModello, m.nomeModello, nm.noleggiModello from noleggiModelli nm JOIN modelli m ON m.idModello=nm.idModello where nm.noleggiModello=(select max(noleggiModello) from noleggiModelli);

|  |  |  |
| --- | --- | --- |
| nomeModello | idModello | noleggiModello |
| La Risorgiva | 1 | 2 |

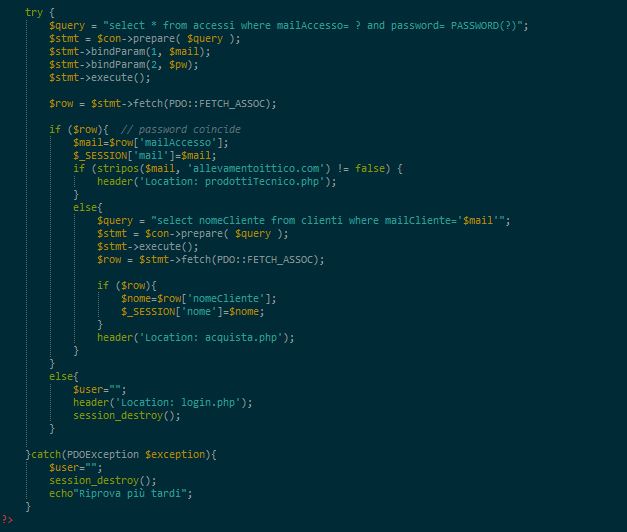
Sito web, visualizzazione prodotti disponibili al noleggio:

Codice significativo:



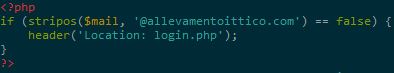
Sito web, login all’area riservata:

Codice significativo:



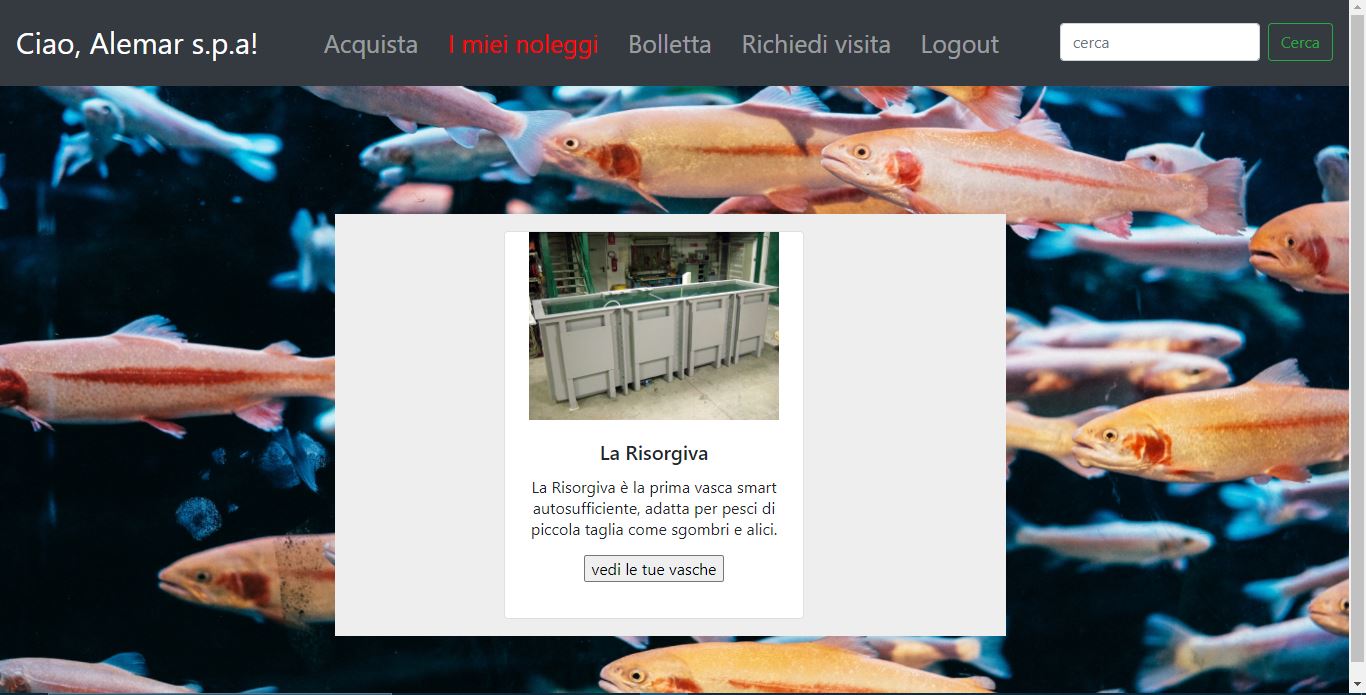
Controllo accessi diversificati per utenti non riconosciuti:

* Dipendenti

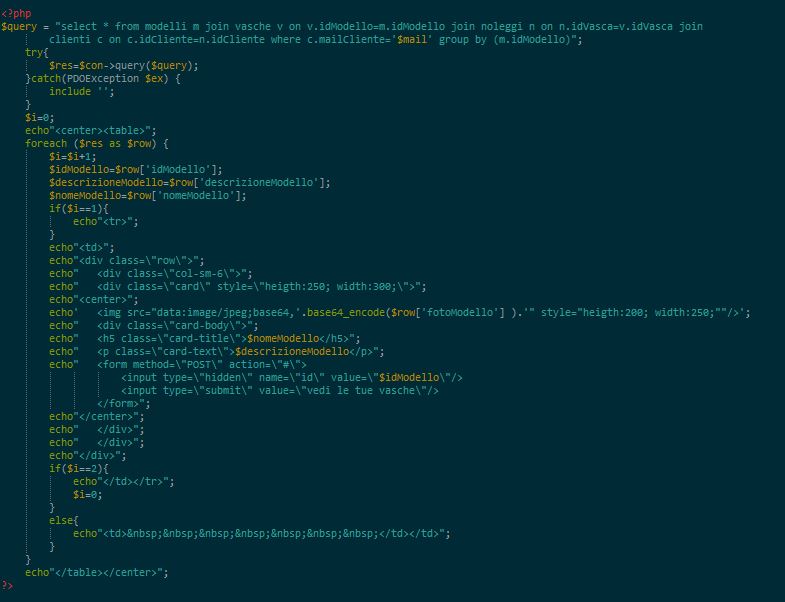


* Clienti

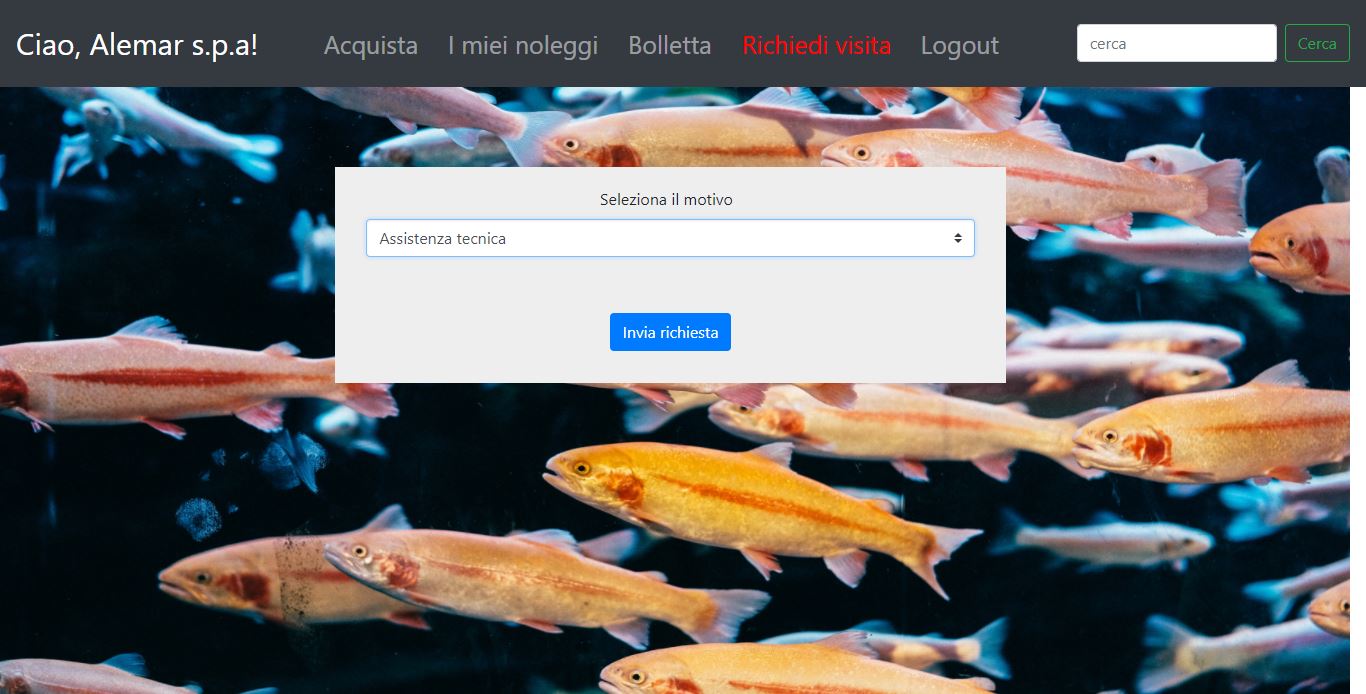


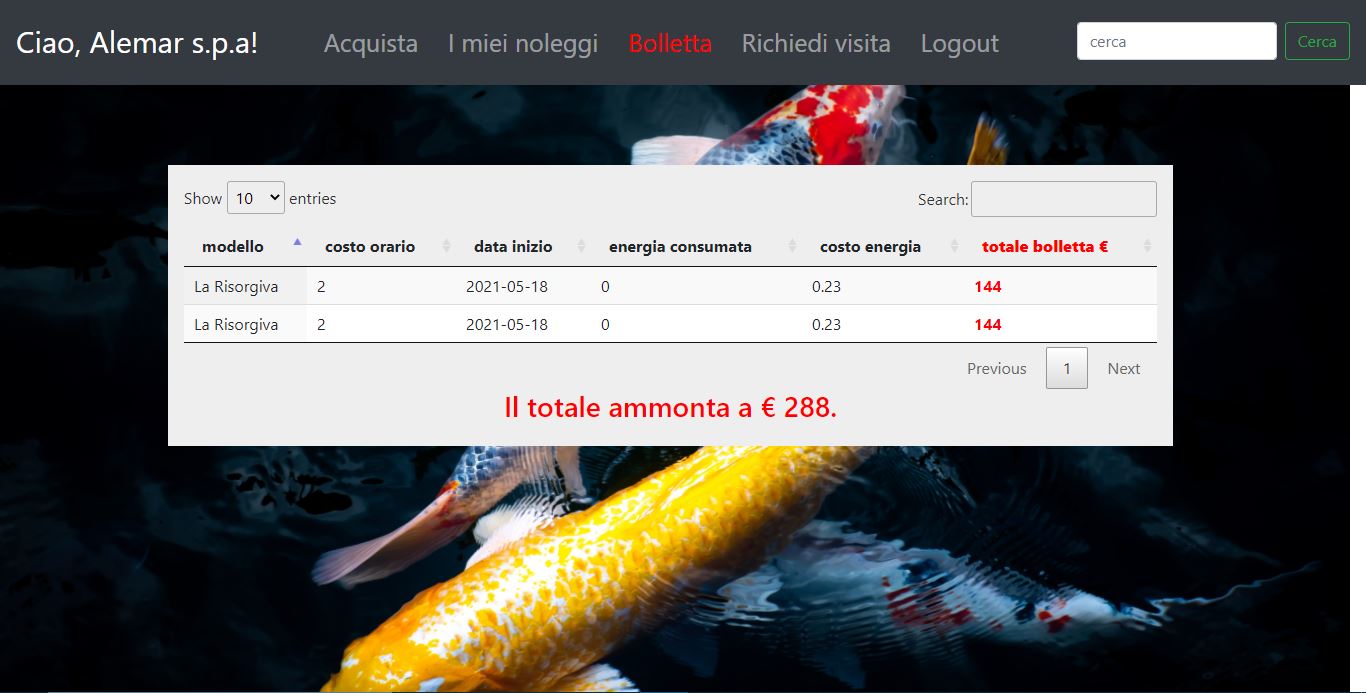
Sito web, area riservata al cliente “Alemar s.p.a.”, panoramica sui noleggi effettuati:

Codice significativo:

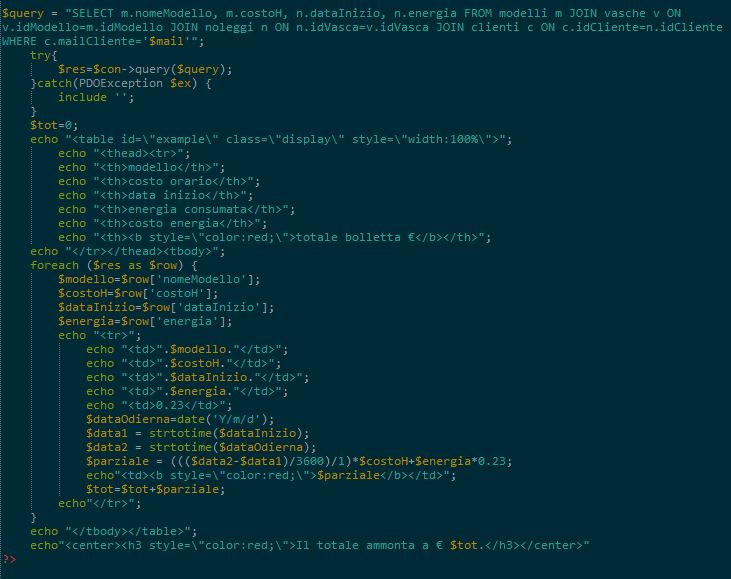


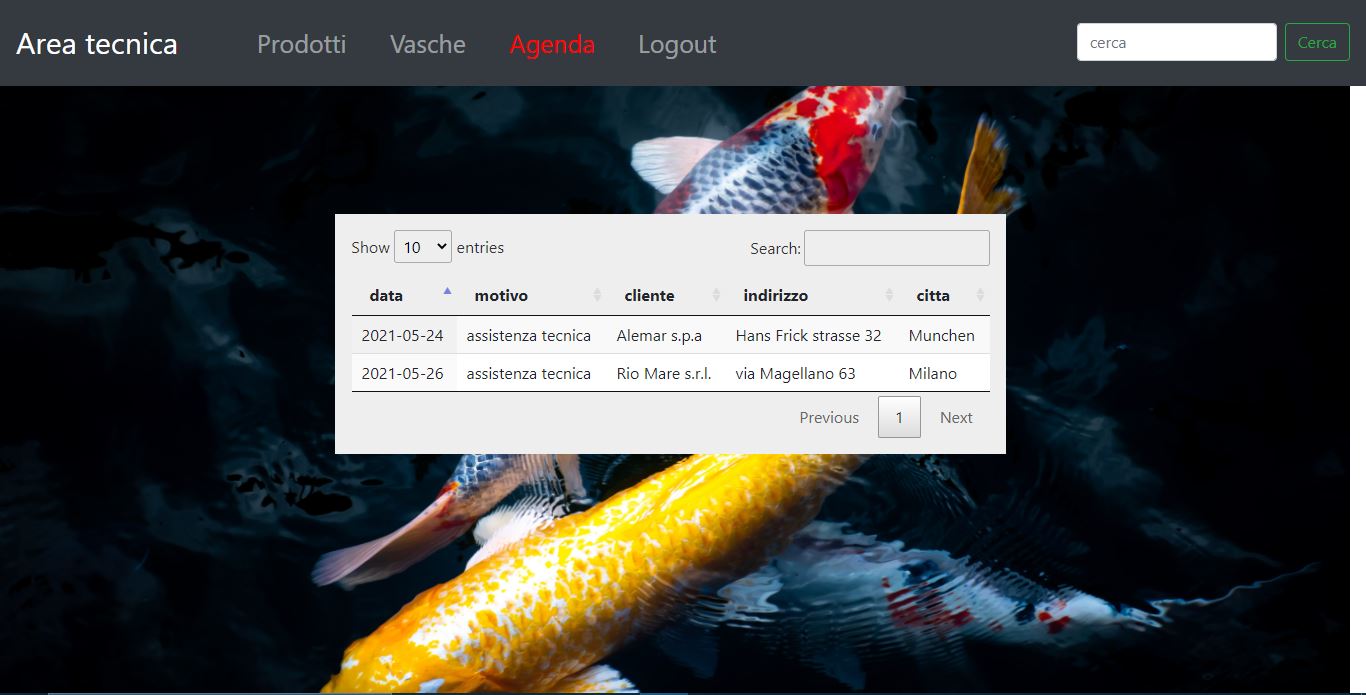
Sito web, area riservata al cliente “Alemar s.p.a”, sezione di richiesta visita tecnico:



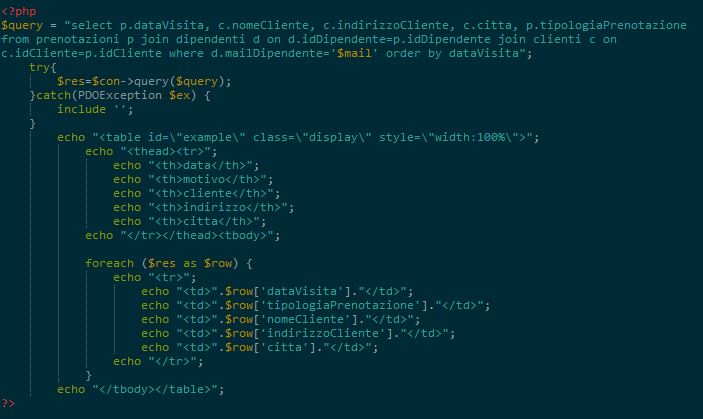
 Sito web, area riservata al cliente “Alemar s.p.a”, sezione di riepilogo costo bolletta:

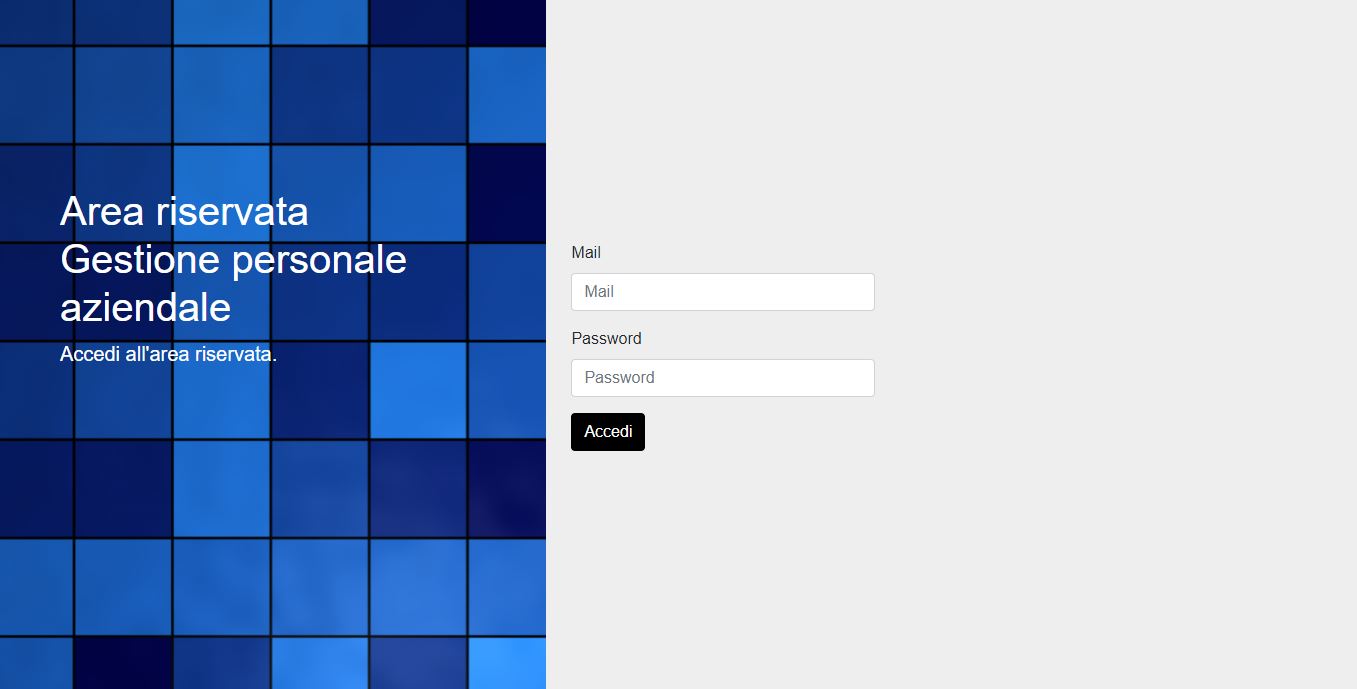
Codice significativo:



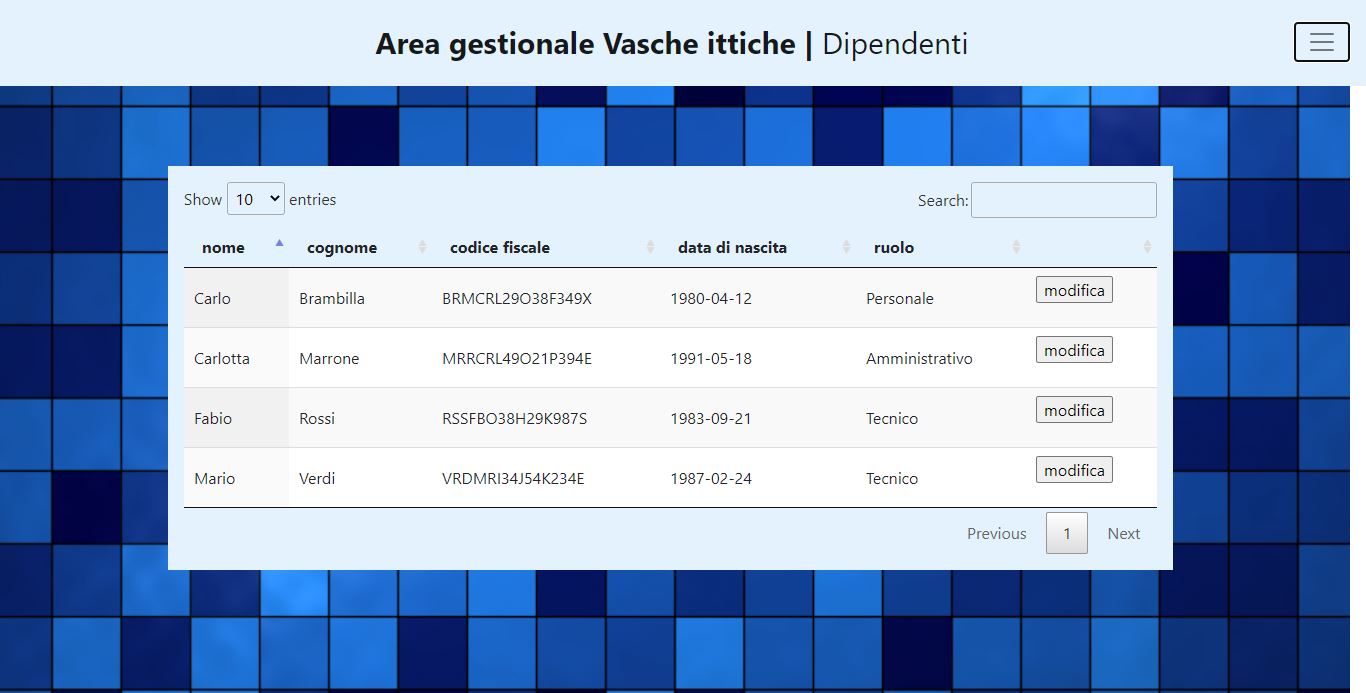
Sito web, area riservata al tecnico “Mario Verdi”, agenda degli impegni:

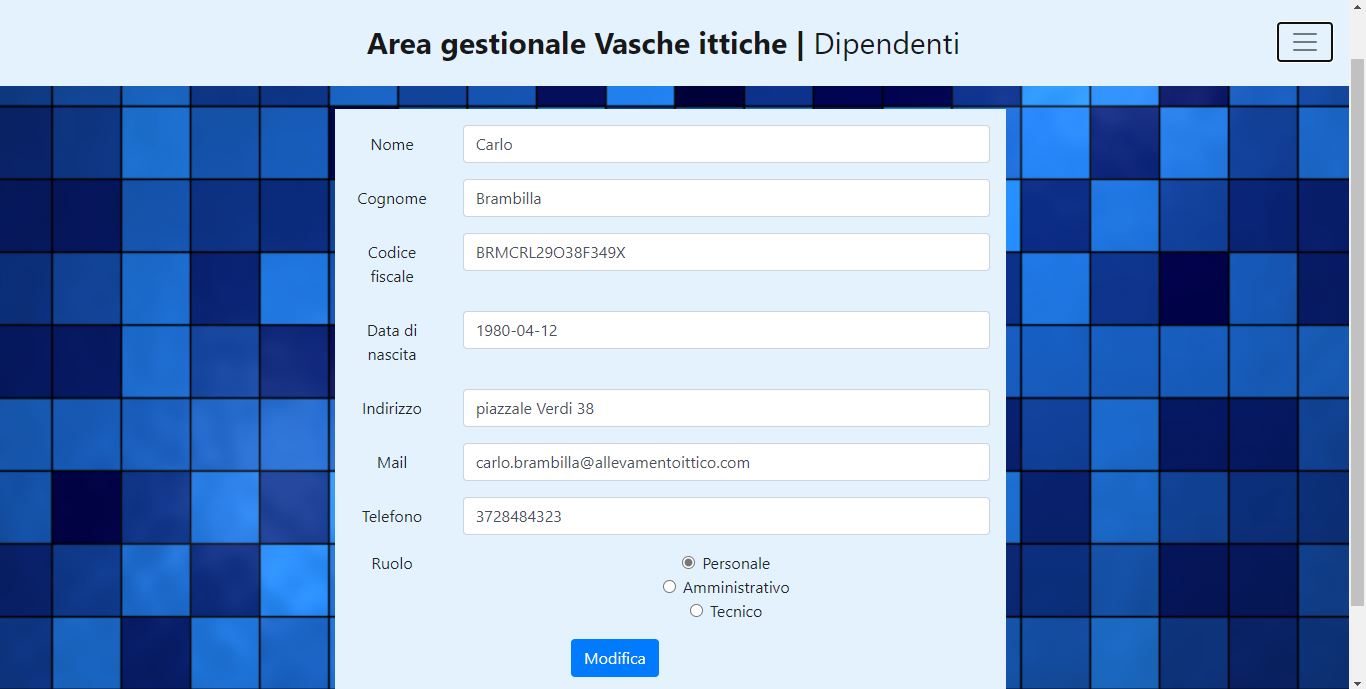
Codice significativo:

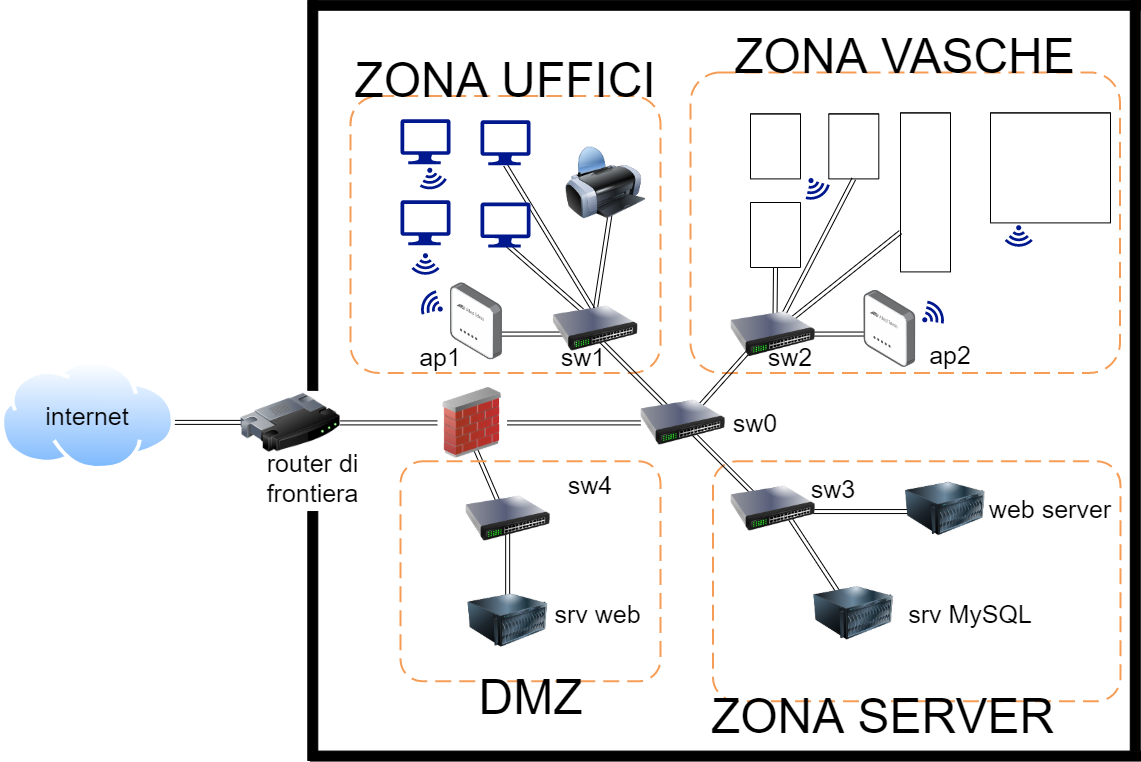


Sito gestionale interno, login:

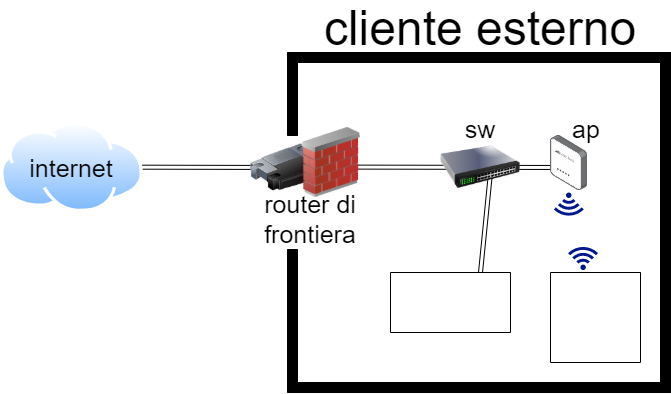
Sito gestionale interno, panoramica sui dipendenti:



Sito gestionale interno, specifica dei dati del dipendente “Carlo Brambilla”:

Infrastruttura di rete interna all’azienda:

Esempio di possibile infrastruttura di rete esterna, posseduta da un cliente:



Infrastruttura di rete interna all’azienda:

Si assume che l’azienda abbia, principalmente, quattro sale tra loro separate, e una connessione internet a banda larga (FTTH) garantita e assicurata. Il dominio e il mail server sono gestiti esternamente da terze parti.

* Zona uffici: una sala, open space, viene dedicata alla zona amministrativa dell’azienda. In questa sala troviamo le diverse postazioni dei dipendenti e il PC del direttore. Oltre alla rete cablata sarà presente un Access Point connesso allo switch di zona per permettere ad utenti esterni o ai clienti di connettersi ad internet. Logicamente verranno implementate due VLAN diverse, una per i PC dei dipendenti (rete Ethernet) e una per il personale esterno (rete Wifi). Nella zona uffici saranno, inoltre, disponibili stampanti di rete connesse alla rete ethernet.
* Zona vasche: la sala più ampia viene dedicata all’esposizione delle vasche presenti in azienda, tutte connesse alla rete internet aziendale tramite rete cablata o rete wireless. Sia le rete ethernet che la rete wireless sono implementate sulla stessa VLAN e sulla stessa rete. Gli indirizzi IP per le vasche connesse alla rete ethernet saranno statici (con un range da .2 a .126), mentre per le vasche connesse tramite wifii l’indirizzamento IP verrà affidato al DHCP del router aziendale che opererà su un range di indirizzi definito (es. da .127 a .254).
* Zona server: questa sala dev’essere in una zona protetta dell’azienda, preferibilmente senza finestre rivolte all’esterno, con temperatura strettamente controllata e accesso tramite smart card con tecnologia RFID in dotazione ai tecnici aziendali più anziani e al direttore. Questa sala deve essere insonorizzata, schermata da interferenze esterne, climatizzata e con umidità controllata. Tutti i server qui presenti apparterranno alla stessa rete e alla stessa VLAN.
* Zona DMZ: come per la zona server anche la zona DMZ, dedicata ai server esposti all’esterno (su internet), deve essere protetta e strettamente controllata; i criteri di sicurezza e i parametri da rispettare sono i medesimi della zona server. Per motivi di sicurezza lo switch di questa zona sarà direttamente e fisicamente collegato al firewall dell’azienda. Tutti i server presenti nella zona DMZ apparterranno alla stessa rete e alla stessa VLAN.
* Vasche noleggiate: per vasche noleggiate da clienti esterni e poste, quindi, in strutture esterne all’azienda è implementata una rete distinta ed una VLAN distinta, che permette l’accesso ai server di gestione delle vasche stesse. Le relative vasche potranno essere collegate alla rete del cliente tramite cavo ethernet o collegamento wireless.

Tra il router di frontiera aziendale e il router di frontiera del cliente è instaurata una connessione VPN site-to-site con tunnel IPSec.

Sistemi hardware e software:

* Dispositivi di rete: per i dispostivi di rete aziendali (router, switch e access point) si è deciso di scegliere una configurazione unica dell’azienda multinazionale CISCO, per la qualità e l’affidabilità la garantita:
  + Router Cisco,
  + Switch Cisco,
  + Access Point Cisco.
* Firewall IP Fire: si è scelto questo tipo di firewall per la facilità d’implementazione e gestione dello stesso.
* Server Linux Apache: per entrambi i web server aziendali si è scelto di utilizzare la distribuzione di Linux Apache. Essendo i sorgenti degli applicativi aziendali scritti in PHP sarà necessario scaricare sui server le relative librerie.
* Server Linux Apache con MySQL: per il database server si è, invece, scelto di utilizzare il software gestionale (DBMS) MySQL. Anche in questo caso sarà necessario scaricare le relative librerie.
* PC HP con windows: il sistema operativo scelto per la realtà aziendale è Windows, per la sua diffusione e immediatezza d’uso anche per utenti non esperti.
* Stampanti HP: per sfruttare al meglio l’ecosistema offerto da HP si è scelto di optare per stampanti HP, direttamente accoppiabili con i PC presenti.
* PHP: sia il sito web aziendale, esposto su internet e presente sul server web in DMZ, che per la web application gestionale, presente sul web server nella zona server interna, è stato scelto come linguaggio di programmazione PHP. Questo perché
  + PHP è compatibile con i motori di ricerca grazie ad alcune delle applicazioni e funzionalità integrate. Avere un sito web ottimizzato per i motori di ricerca aiuta a possedere un buon posizionamento del sito aziendale nei motori di ricerca. I siti con un posizionamento elevato nei motori di ricerca, infatti, godono di un traffico più elevato, elemento fondamentale per un’azienda.
  + PHP ha funzionalità di sicurezza integrate che rendono i siti web creati con esso molto sicuri e protetti da attacchi informatici, minacce e virus. Può anche essere facilmente ridimensionato e crittografato.
  + Un altro importante puntoa favore dell’uso di PHP è il livello di flessibilità, robustezza e scalabilità integrato in PHP stesso. Rispetto ad altri linguaggi, il più grande vantaggio di PHP è che il codice del sito web può essere aggiornato senza richiedere il riavvio del server.
  + L’aspetto grafico dell’applicazione è facilmente implementabile tramite CSS e script JAVASCRIPT, integrati con PHP.

Servizi e configurazioni:

* Piano di indirizzamento: per l’indirizzamento IP aziendale si è scelto di utilizzare reti ben distinte e riconoscibili facilmente in caso di problemi di vario genere e con un’ampia disponibilità di host assegnabili; come già anticipato, l’azienda verrà divisa in quattro zone fisiche distinte:
  + Zona uffici: la zona uffici verrà logicamente divisa in due reti distinte, una cablata dedicata ai PC dei dipendenti e una wireless con accesso con protocollo WPA3 Personal dedicata ai clienti o al personale esterno dell’azienda:
    - UFFICI:= 192.168.10.0 /24
    - WIFI UFFICI:= 192.168.20.0 /24
* Zona vasche: la zona vasche permette l’accesso sulla rete gestionale aziendale delle vasche esposte sia tramite rete cablata che tramite rete wireless:
  + VASCHE:= 192.168.30.0 /24

L’indirizzamento IP delle vasche connesse tramite ethernet viene gestito staticamente, assegnando un range di indirizzi da .2 a .126; per le vasche connesse tramite rete wireless viene usato il DHCP interno del router aziendale, che assegnerà alle vasche gli indirizzi IP nel range tra .127 a .254.

Le vasche noleggiate dai clienti e, quindi, poste in reti esterne, una volta connesse al router del cliente tramite rete cablata o wireless instaureranno una vpn site-to-site con la rete aziendale e vi accederanno con una rete dedicata:

* + VASCHE ESTERNE:= 192.168.30.0 /24
* Zona server: i server aziendali non esposti esternamente sulla rete internet appartengono ad una stessa rete cablata:
  + SERVER:= 192.168.99.0 /24
* Zona DMZ: nella zona DMZ sarà presente il web server ospitante il sito web e la web application dell’azienda raggiungibile dalla rete internet:
  + DMZ:= 172.16.0.0 /24
  + VLAN: si è, inoltre, scelto di implementare le VLAN per facilitare l’implementazione della rete aziendale, per garantire maggiore sicurezza e per gestire più facilmente futuri cambiamenti topologici aziendali. Le reti VLAN sono così assegnate:
    - VLAN UFFICI:= 192.168.10.0 /24
    - VLAN WIFI UFFICI:= 192.168.20.0 /24
    - VLAN VASCHE:= 192.168.30.0 /24
    - VLAN VASCHE ESTERNE:= 192.168.40.0 /24
    - VLAN SERVER:= 192.168.99.0 /24
    - VLAN DMZ:= 172.16.0.0 /24

Con l’utilizzo delle VLAN sarà necessario implementare i relativi servizi su switch e router aziendali. La connessione tra il router aziendale e lo switch stella sarà posta in modalità trunk, tutte le altre connessioni saranno, invece, in modalità access.

* Access Point - WPA3 Personal: sia nella zona uffici che nella zona vasche sono presenti access point:
  + - Access Point zona uffici: gli Access Point qui presenti utilizzano un protocollo di crittografia WPA3-Personal, ottimizzato per piccole reti. Gli utenti potranno connettersi al wifi aziendale tramite questi Access Point inserendo una password unica.
    - Access Point zona vasche: gli Access Point presenti in questa zona utilizzano, anch’essi, una crittografia di tipo WPA3-Personal, che, tramite l’inserimento di una password, permettono alle vasche di accedere alla rete unica a loro dedicata (che sia cablata o wireless).
* Router di frontiera: si assume che l’azienda disponga di un indirizzo IP pubblico statico, di conseguenza il servizio di DNS viene gestito esternamente dalla stessa azienda fornitrice del dominio dell’azienda. Stesso discorso applicabile per il servizio di mail server aziendale SMTP, per assicurare una maggiore affidabilità e una migliore gestione professionale del servizio stesso. L’istanza server SMTP acquistata dall’azienda offre a quest’ultima una mail aziendale e la possibilità di assegnare una mail aziendale personale ad ogni dipendente dell’azienda, con la quale potrà, poi, accedere ai servizi riservati aziendali.

Sono, inoltre, implementati i seguenti servizi:

* + PAT: per le connessioni dall’interno all’esterno è necessario implementare un servizio PAT, evoluzione del servizio destination NAT, che permette a più utenti di aprire molteplici connessioni sulla rete internet esterna tramite mappature tra più [indirizzi IP](https://it.wikipedia.org/wiki/Indirizzo_IP) di una  e un singolo indirizzo IP di una rete pubblica sfruttando le porte di apertura delle connessioni.
  + Port Forwarding: per le connessioni dall’esterno all’interno è necessario implementare il servizio di Port Forwarding. In particolare è necessario implementare questo servizio sulla porta 443 del server web posto nella DMZ.
  + DHCP: per gestire l’indirizzamento IP degli host connessi tramite rete wireless si è scelto di implementare il servizio di DHCP del router. Come anticipato, le vasche connesse in modalità wireless disporranno di un range di indirizzi IP da 192.168.30.127 a 192.168.30.254. Gli utenti connessi al Wifi aziendale disporranno, invece, di un range di indirizzi IP da 192.168.20.2 a 192.168.20.254.
  + NAS: per gestire l’accesso da remoto delle vasche noleggiate dai clienti e poste su reti esterne è necessario implementare le VPN site-to-site in modalià tunnel IPSec. Un servizio da implementare per il corretto funzionamento delle relative VPN è il NAS, che permette l’accesso agli “utenti” autorizzati.
  + VLAN: l’implementazione delle VLAN è stata scelta per facilitare l’implementazione della rete aziendale, per garantire maggiore sicurezza e per gestire più facilmente futuri cambiamenti aziendali interni. Con l’utilizzo delle VLAN è necessario porre in modalità trunk la connessione tra il router aziendale e lo switch stella presente in azienda, mentre tutte le altre connessioni saranno poste in modalità access.
* Database server:
* MySQL: il server database ha installato come DBMS MySQL, per poter implementare ampie strutture di dati e disporre di una facile gestione generale del database stesso.
* Firewall:
  + Packet Filtering: il firewall scelto dall’azienda è IP Fire, di tipo packet filtering con le seguenti ACL implementate:

VLAN UFFICI:= 192.168.10.0 /24

VLAN WIFI UFFICI:= 192.168.20.0 /24

VLAN VASCHE:= 192.168.30.0 /24

VLAN VASCHE ESTERNE:= 192.168.40.0 /24

VLAN SERVER:= 192.168.99.0 /24

VLAN DMZ:= 172.16.0.0 /24

INTERNET:= NOT (VLAN UFFICI, VLAN WIFI UFFICI, VLAN VASCHE, VLAN VASCHE ESTERNE, VLAN SERVER, VLAN DMZ)

VLAN UFFICI -> VLAN SERVER

www, ssh, mysql

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VERSO | IP SORG | IP DEST | PROTOCOL | PORTA S. | PORTA D. | FLAG | AZIONE |
| OUT | uffici | server | TCP | >1023 | 80,443 | 0/1 | PERMIT |
| IN | server | uffici | TCP | 80,443 | >1023 | 1 | PERMIT |
| OUT | uffici | server | TCP | >1023 | 22 | 0/1 | PERMIT |
| IN | server | uffici | TCP | 22 | >1023 | 1 | PERMIT |
| OUT | uffici | server | TCP | >1023 | 3306 | 0/1 | PERMIT |
| IN | server | uffici | TCP | 3306 | >1023 | 1 | PERMIT |
| Any | Any | Any | Any | Any | Any | \* | DENY |

VLAN VASCHE -> VLAN SERVERmysql

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VERSO | IP SORG | IP DEST | PROTOCOL | PORTA S. | PORTA D. | FLAG | AZIONE |
| OUT | vasche | server | TCP | >1023 | 3306 | 0/1 | PERMIT |
| IN | server | vasche | TCP | 3306 | >1023 | 1 | PERMIT |
| Any | Any | Any | Any | Any | Any | \* | DENY |

VLAN VASCHE ESTERNE-> VLAN SERVER

mysql

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VERSO | IP SORG | IP DEST | PROTOCOL | PORTA S. | PORTA D. | FLAG | AZIONE |
| OUT | vasche ext | server | TCP | >1023 | 3306 | 0/1 | PERMIT |
| IN | server | Vasche ext | TCP | 3306 | >1023 | 1 | PERMIT |
| Any | Any | Any | Any | Any | Any | \* | DENY |

VLAN UFFICI -> VLAN DMZ

www,ssh

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VERSO | IP SORG | IP DEST | PROTOCOL | PORTA S. | PORTA D. | FLAG | AZIONE |
| OUT | uffici | server | TCP | >1023 | 80,443 | 0/1 | PERMIT |
| IN | server | uffici | TCP | 80,443 | >1023 | 1 | PERMIT |
| OUT | pc presid | server | TCP | >1023 | 22 | 0/1 | PERMIT |
| IN | server | pc presid | TCP | 22 | >1023 | 1 | PERMIT |
| Any | Any | Any | Any | Any | Any | \* | DENY |

VLAN WIFI UFFICI -> VLAN DMZ

www

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VERSO | IP SORG | IP DEST | PROTOCOL | PORTA S. | PORTA D. | FLAG | AZIONE |
| OUT | uffici | server | TCP | >1023 | 80,443 | 0/1 | PERMIT |
| IN | server | uffici | TCP | 80,443 | >1023 | 1 | PERMIT |
| Any | Any | Any | Any | Any | Any | \* | DENY |

VLAN DMZ -> VLAN SERVER

mysql

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VERSO | IP SORG | IP DEST | PROTOCOL | PORTA S. | PORTA D. | FLAG | AZIONE |
| OUT | dmz | server | TCP | >1023 | 3306 | 0/1 | PERMIT |
| IN | server | dmz | TCP | 3306 | >1023 | 1 | PERMIT |
| Any | Any | Any | Any | Any | Any | \* | DENY |

RETE INTERNET -> VLAN DMZ

www

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VERSO | IP SORG | IP DEST | PROTOCOL | PORTA S. | PORTA D. | FLAG | AZIONE |
| OUT | internet | server | TCP | >1023 | 443 | 0/1 | PERMIT |
| IN | server | internet | TCP | 443 | >1023 | 1 | PERMIT |
| Any | Any | Any | Any | Any | Any | \* | DENY |

VLAN UFFICI -> RETE INTERNET

www

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VERSO | IP SORG | IP DEST | PROTOCOL | PORTA S. | PORTA D. | FLAG | AZIONE |
| OUT | uffici | internet | TCP | >1023 | 80,443 | 0/1 | PERMIT |
| IN | internet | uffici | TCP | 80,443 | >1023 | 1 | PERMIT |
| Any | Any | Any | Any | Any | Any | \* | DENY |

VLAN WIFI UFFICI -> RETE INTERNET

www

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VERSO | IP SORG | IP DEST | PROTOCOL | PORTA S. | PORTA D. | FLAG | AZIONE |
| OUT | uffici wles | internet | TCP | >1023 | 80,443 | 0/1 | PERMIT |
| IN | internet | uffici wles | TCP | 80,443 | >1023 | 1 | PERMIT |
| Any | Any | Any | Any | Any | Any | \* | DENY |

* Connessione da remoto alla rete aziendale da parte delle vasche noleggiate:
  + VPN site-to-site con suite IPSec protetta in modalità tunnel: per le VPN di tipo site-to-site è stata scelta la suite di protocolli IPSec, di livello rete, protetta in modalità tunnel, aggiungendo un livello di sicurezza con l’incapsulamento al fine di proteggere ogni pacchetto nel suo viaggio su internet. Lo scambio di chiavi è implementato tramite il protocollo IKE; viene poi utilizzato il protocollo ESP per garantire confidenzialità, integrità e autenticazione. L’accesso alla rete aziendale interna verrà regolamentata dal servizio NAS del router aziendale.
* Certificato digitale: per implementare il sito web aziendale esposto su internet è necessario richiedere il certificato digitale ad un ente di certificazione riconosciuto (CA), dopo aver creato la chiave pubblica e la chiave privata del web server in questione.

Comunicazione:

* Piano di indirizzamento:
  + VLAN UFFICI:= 192.168.10.0 /24
  + VLAN WIFI UFFICI:= 192.168.20.0 /24
  + VLAN VASCHE:= 192.168.30.0 /24
  + VLAN VASCHE ESTERNE:= 192.168.40.0 /24
  + VLAN SERVER:= 192.168.99.0 /24
  + VLAN DMZ:= 172.16.0.0 /24
* Protocolli di comunicazione:
  + HTTP over TLS: il protocollo di comunicazione utilizzato all’interno dell’azienda è HTTP over TLS. Essendo HTTP un protocollo stateless, di livello applicazione, che permette la comunicazione tra client e server web, nell’applicativo aziendale saranno usate le sessioni, per offrire una migliore esperienza d’utilizzo all’utente e facilitare l’implementazione di servizi di sicurezza da parte degli sviluppatori. Ad ogni login, quindi, verrà cominciata una sessione dedicata dell’utente, che verrà terminata solo quando verrà effettuato il logout.
  + SSH: viene implementato il protocollo SSH per poter gestire e implementare servizi sui server interni, stabilendo una [sessione](https://it.wikipedia.org/wiki/Sessione) remota [cifrata](https://it.wikipedia.org/wiki/Crittografia) tramite [interfaccia a riga di comando](https://it.wikipedia.org/wiki/Interfaccia_a_riga_di_comando).

Ulteriori scelte implementative:

* Tablet aziendali: i tecnici dell’azienda vengono dotati di tablet con connessione ad internet 4G. Quest’ultimi vengono usati a scopo lavorativo quando un tecnico è chiamato ad assistere un cliente o, semplicemente, per controllare lo stato di una vasca in ogni momento, in prontezza e semplicità.
* Privacy dei dati sensibili: visto il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 è obbligatorio proteggere e non raccogliere i dati sensibili personali a scopo di lucro. Conseguentemente a ciò, prima di una nuova registrazione verrà chiesto agli utenti di leggere le condizioni d’uso dei dati personali da parte dell’azienda e di confermare l’avvenuta lettura e consenso all’uso stesso dei dati. Ogni 3 mesi (o al primo accesso dell’utente dopo 3 mesi dall’ultima volta) verrà richiesto agli utenti di cambiare password, che dovrà essere diversa dalla precedente utilizzata. I dati sulle azioni degli utenti, memorizzati nella tabella *Log* del database aziendale, all’interno dell’area riservata verranno conservati per una durata di 6 mesi a scopo preventivo.
* PC del direttore:
  + TeamViewer: nella zona uffici è presente la postazione del direttore e ogni PC presente avrà installato TeamViewer; TeamViewer preferisce effettuare connessioni TCP e UDP in uscita sulla porta 5938: questa è la porta principale che utilizza e TeamViewer offre prestazioni migliori utilizzando questa porta. Nel personal firewall del PC del direttore, quindi, verrà consentito l’utilizzo di questa porta in uscita ma non in entrata, mentre in tutti gli altri PC presenti della zona uffici sarà concessa l’apertura delle relative porte in entrata. Se TeamViewer non riesce a connettersi sulla porta 5938, proverà a connettersi sulla porta TCP 443. Così facendo solo il direttore potrà aprire connessioni remote tramite Teamviewer.
  + Veyon: ugualmente a TeamViewer, su ogni PC presente nella zona uffici verrà installato il software Veyon per la possibilità di controllare ogni singolo PC da remoto e per poter trasmettere sui PC dei dipendenti schemi e informazioni utili a seconda delle situazioni. Anche in questo caso sarà necessario aprire le porte 11100 e 11400 dei personal firewall dei PC presenti nella zona uffici e consentendo l’apertura di connessione dal PC del direttore e negando i tentativi di connessione in entrata ad esso. Per tutti gli altri PC presenti della zona uffici sarà concessa l’apertura delle relative porte in entrata.