Revista Perspectivas Online: Exatas & Engenharia
Dezembro/2024, v.15 , n.39, p.37- 48
ISSN: 2236-885X (Online)
DOI: 10.25242/885X153920243058

USO DE RECONHECIMENTO FACIAL NO CONTROLE DE ACESSO AO ISECENSA

Lucélio Dias de Azevedo[1], Luiz Cláudio Vieira [2], Luiz Eduardo Dias Ribeiro [3]

RESUMO

AZEVEDO, L. D.; VIEIRA, L. C.; RIBEIRO, L. E. D.; Uso de Reconhecimento Facial no Controle de Acesso ao ISECENSA. **Perspectivas Online: Exatas & Engenharia**, v. 15 , n. 39, p.37-48, 2024.

Segurança é fator primordial para qualquer instituição. No caso de instituições de ensino, devido ao alto fluxo de circulação de pessoas, elas tem o desafio de proteger não só alunos, mas também funcionários e professores. Esse tipo de ambiente deve possuir monitoramento constante, afim de garantir que somente indivíduos autorizados tenham acesso. O ISECENSA utilizava inicialmente identificação por cartões de acesso com código de barras e posteriormente, biometria por digital. Lentidão, filas e reclamações eram comuns no contexto do dia-a-dia da portaria. A identificação biométrica é definida como uma maneira de identificar e autenticar usuários. No contexto da instituição de ensino, a identificação por reconhecimento facial foi escolhida pois entregava dois itens fundamentais: segurança e agilidade. Como a instituição utiliza diferentes sistemas, foram criados os chamados “webservices”, que retornam informações específicas e detalhadas dos usuários do sistema. Por fim, o trabalho demonstra em números como a biometria facial agilizou o processo de identificação e autorização dos usuários.

Palavras-chave: Biometria; Identificação; Face; Rosto.

[1] Analista de Sistemas – ISECENSA. Doutorando em Modelagem e Tecnologia para o Meio Ambiente Aplicadas em Recursos Hídricos – Instituto Federal Fluminense, Brasil;
[2] Professor – ISECENSA. Especialista em Administração em Redes Linux – UFLA, Brasil.
[3] Supervisor de Suporte de Sistemas – CENSA, Brasil.
(*) e-mail: lucelio.azevedo@isecensa.edu.br

Data de recebimento: 06/11/2024 Aceito para publicação: 18/11/2024 Data de publicação: 21/05/2025

Online Perspectives: Exact and Engineering
December/2024, v.15 , n.39 , p.37-48
ISSN: 2236-885X (Online)
DOI: 10.25242/885X153920243058

USE OF FACIAL RECOGNITION IN ACCESS CONTROL TO ISECENSA

Lucélio Dias de Azevedo[1], Luiz Cláudio Vieira [2], Luiz Eduardo Dias Ribeiro [3]

ABSTRACT

AZEVEDO, L. D.; VIEIRA, L. C.; RIBEIRO, L. E. D.; Use of Facial Recognition in Access Control to ISECENSA. **Online Perspectives: Exact and Engineering**, v. 15, n. 39, p. 37-48, 2024.

Security is a primary factor for any institution. In the case of educational institutions, due to the high flow of people, they have the challenge of protecting not only students, but also employees and teachers. This type of environment must be constantly monitored to ensure that only authorized individuals have access. ISECENSA initially used identification by access cards with bar codes and later, biometrics by fingerprint. Slowness, queues and complaints were common in the context of the day-to-day life of the concierge. Biometric identification is defined as a way to identify and authenticate users. In the context of the educational institution, facial recognition identification was chosen because it delivered two fundamental items: security and agility. As the institution uses different systems, the so-called "webservices" were created, which return specific and detailed information from the users of the system. Finally, the work demonstrates in numbers how facial biometrics has streamlined the process of identifying and authorizing users.

Keywords: Biometrics; Identification; Face, Recognition.

[1] Systems Analyst – ISECENSA. Student of Doctoral Program in Modeling and Technology for the Environment Applied to Water Resources – Fluminense Federal Institute, Brazil;
[2] Professor – ISECENSA. Linux Network Administration Specialist – UFLA, Brazil.
[3] Systems Support Supervisor – CENSA, Brazil.
(*) e-mail: lucelio.azevedo@isecensa.edu.br

Received: 06/11/2024 Accepted: 18/11/2024 Published online: 21/05/2025

1. INTRODUÇÃO

Nos dias atuais, a segurança é fator primordial para qualquer instituição. No caso de instituições de ensino, não só a proteção dos alunos, mas também de funcionários e visitantes é um desafio, e os avanços da tecnologia podem ajudar a reduzir e/ou prever os possíveis problemas. O contexto dinâmico do ambiente de instituições de ensino, com a circulação constante de pessoas, deve possuir monitoramento constante afim de evitar que indivíduos não autorizados tenham acesso.

Utilizando essa premissa para controle, (SOUZA, 2010) entende que são necessários estebelecer perímetros que possuam acesso isolado, utilizando barreiras físicas e tecnologias de deteção, focando na identificação do indivíudo tanto na entrada quanto na saída.

A identificação biométrica é definida por (MISSINI e LAJÇI, 2022) como uma maneria de identificar e autenticar usuários, onde um aspecto característico único de uma pessoa (como digitais, rosto, voz, dna, olhos, assinatura, por exemplo) é usado para realizar a autenticação. Essas características tem diversas vantagens, como: unicidade (é único), permanência (não muda, sendo estável durante muito tempo), coletabilidade (facilmente adquirida por metodos não intrusivos), performance (alto nível de acurácia com baixa quantidade de falsos-positivos), aceitação (socialmente e culturalmente aceitáveis), anti-evasão (dificuldade de burlar), interomperabilidade (funciona com diferentes tipos de dispositivos e sistemas).

O trabalho de (CHOWDHURY et. al., 2017) afirma que autenticações biométricas estão se tornando o muito populares e o reconhecimento do rosto humano e uma técnica que se comparada a outros tipos de biometria, podendo até reconhecer de maneira não intrusiva, sujeitos que não estão cooperando com a identificação. Os autores apontaram 2 (dois) problemas comuns para o reconhecimento facial: depender de iluminação apropriada e uso expressões faciais. Estes são dois infortúnios que podem diminuir a confiabilidade do reconhecimento. (ITPRO, 2024) ainda cita como vantagens da identificação facial sua agilidade e melhor segurança: não há como alguém entregar sua identificação facial para outra pessoa, assim, somente a pessoa autorizada irá acessar o ambiente em questão. A pessoa precisa apenas posicionar o rosto em frente a uma câmera para que o dispositivo identificador o reconheça e faça a autorização do acesso.

O ISECENSA utilizava inicialmente catracas com o tipo de identificação por cartões de acesso com códigos de barra, sendo necessário renová-los a cada semestre. Posteriormente, foi utilizado o serviço de identificação por biometria digital, que tinha problemas como lentidão ou não reconhecimento da digital do usuário (o mesmo não posicionava o dedo corretamente, ou sua digital estava deteriorada por qualquer motivo), e frequentemente aconteciam grandes filas que atrasavam a entrada dos usuários, gerando reclamações. Como as catracas estão localizadas em ambiente interno e iluminado e a coleta de fotos é feita de maneira controlada, decidiu-se pelo uso do reconhecimento facial como forma de identificação e autorização. Foi escolhido o modelo iDFace (ControlID, 2024), que é um dispositivo com tela touch e software embarcado para deteção de rostos, podendo ser cadastradas até 10.000 faces.

Para consultar as informações dos alunos, funcionários e visitantes que terão autorização de acesso à instituição, são usados webservices. (MOHANTHY e PATTNAIK, 2019) descrevem um webservice como um processo fracamente acoplado (não dependente de outros processos) e acessível via internet, que entrega informações sem precisar conhecer seus

consumidores (aqueles que efetivamente usam o serviço), o que facilita também a integração de novos consumidores. Identificar serviços e isolar a entrega de informação é um dos maiores desafios no processo de desenvolvimento de um webservice. Neste caso, os webservices consultam os bancos de dados da instituição afim de verificar se o usuário atende as regras de acesso e possui (ou não) alguma restrição.

Este trabalho tem como objetivo geral realizar um estudo de caso acerca do controle de acesso aos Institutos Superiores de Ensino do CENSA - ISECENSA, fazendo um levantamento dos hardwares (parte física) e softwares utilizados, bem como descrever os processos de forma simplificada e direta. Por fim, mostrar como a identificação por biometria facial agilizou o processo de identificação e autorização e reduziu filas e reclamações dos usuários, além de garantir mais segurança para quem frequenta a instituição.

2. METODOLOGIA

Neste estudo de caso, verificou-se que a solução foi implementada utilizando hardwares que podem ser encontrados no mercado de varejo nacional. Já na questão dos softwares integradores, os mesmos foram escritos de maneira personalizada, atendendo exatamente as necessidades e regras da instituição, utilizando as principais linguagens de programação existentes, visando reduzir custos com licenças ou compra de novos módulos integradores. Sendo assim, aproveitando as catracas existentes na portaria do ISECENSA, foram integrados os dispositivos de reconhecimento facial e desenvolvidos softwares que atendessem as regras de negócio da instituição.

2.1 CATRACAS:

As catracas são dispositivos para controle de passagem de pessoas, normalmente instalados em recepções. Tem a vantagem de possuir controle giratório com braços mecânicos, o que impede que uma pessoa não autorizada aproveite a passagem da anterior (GALHARDO, 2011). (PINHEIRO, 2008) diz que as catracas também podem ser definidas como dispositivos físicos que tem o objetivo de permitir que somente usuários autorizados tenham acesso ao ambiente.

O uso de catracas é realizado em diversos segmentos do mercado, e sua adoção, segundo (TOPDATA, 2024), garante segurança dos usuários e permite somente a entrada de pessoas autorizadas. As catracas funcionam como uma barreira física para o usuário. Somente usuários autorizados tem entrada e saída garantidaos, diminuindo o risco de invasões ou atividades ilicitas por conta de terceiros. As catracas eletrônicas da fabricante TopData (Figura 1) já eram utilizadas pela instituição, porém, com a identificação via cartão de acesso e posteriormente, por biometria digital.

Figura 1: Catraca TopData Revolution 4.

2.2 IDENTIFICADOR FACIAL:

Conforme informado por (AMER et. al, 2024), já no ano de 2016 os fabricantes iniciaram estudos sobre fechaduras inteligentes com reconhecimento facial. Essa inovação continuou crescendo em diversos dispositivos tecnológicos, como o iPhone, por exemplo. E essa diversidade de dispositivos adiciona conveniência e segurança, além de facilidade. Com mais fabricantes de dispositivos integrando soluções de idenficação facial aos seus produtos, a tecnologia evolui e se torna mais acessível no mercado.

O dispositivo iDFace (Figura 2), do fabricante Control ID (Control ID, 2024) foi escolhido pois o mesmo possui capacidade de identificar até 10.000 faces, além de possuir display touchscreen e duas câmeras para o reconhecimento, podendo ainda pode ser integrado com relativa facilidade as catracas do fabricante TopData.

Figura 2: Dispostivo IdFace.

2.3 WEBSERVICES:

(MEDURI, 2018) menciona que werbservices tem se tornado um mecanismo para projetar, construir e consumir informações de aplicações, pois organiza tudo de forma que os mesmos possam interagir com outros, priorizando o baixo acoplamento (pouca ou nenhuma dependência de outro serviço) e alta coesão (responsabilidade única e bem definida), facilitando a comunicação entre sistemas heterogêneos.

Foram criados 3 diferentes webservices que retornam informações dos usuários que terão acesso à instituição:

- O primeiro, atende diretamente ao dispositivo identificador.
- O segundo, busca informações no ERP (*Enterprise Resource Planning*, ou, Sistema de Gestão Integrado, em português) TOTVS (TOTVS, 2024), utilizado para controle geral da instituição.
- O terceiro, retorna informações do sistema que controla visitantes e funcionários terceirizados.

São realizadas consultas personalizadas em todos os bancos de dados utilizados, garantindo que a informação permaneça centralizada no que se diz respeito ao controle de acesso: alunos matriculados, alunos com matrícula trancada, alunos que já cursaram, funcionários admitidos, funcionários demitidos, visitantes, etc.

Todas as informações inseridas ou atualizadas nos sistemas são replicadas para as catracas em tempo real, garantindo que o acesso dos usuários seja controlado de forma precisa. A Figura 3 exibe os exemplos de retorno de um webservice para um usuário com permissão e outro com restrições de acesso.

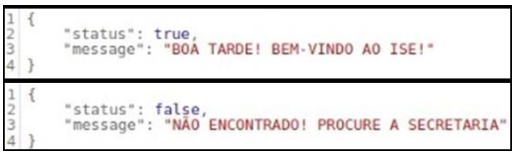


Figura 3 : Exemplos de retorno de webservice.

2.4 SISTEMA DE ACESSO:

Para o acesso de visitantes externos, ou qualquer outra pessoa que não possua vínculo direto com o ISECENSA, foi desenvolvido um sistema para uso nas recepções / portarias da instituição, onde são coletadas informações básicas como nome, e-mail, cpf e telefone, além de uma foto, conforme mostrado na Figura 4. Este mesmo sistema controla o acesso de funcionários terceirizados da instituição, onde os mesmos são cadastrados e vinculados à uma empresa prestadora de serviço.

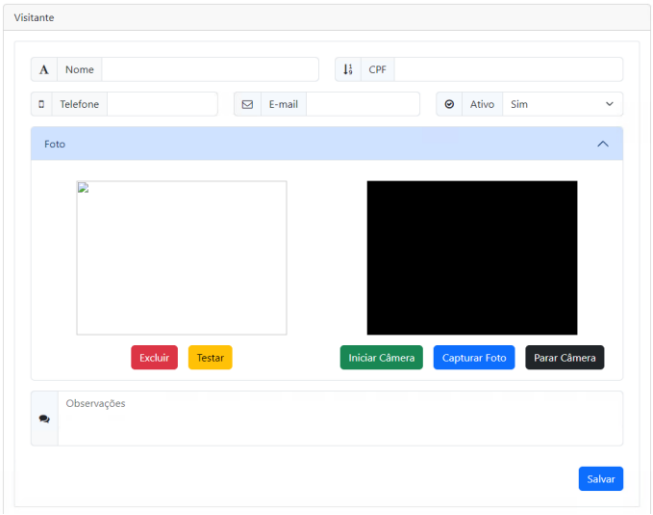


Figura 4 : Tela de cadastro de Visitante.

Quando uma visita é cadastrada, a foto do visitante é enviada para as catracas. A integração do sistema de acesso com os dispositivos idFace foi implementada e as fotos dos usuários externos, no momento do cadastro são testadas e validadas antes de serem guardadas no banco de dados. Também, afim de agilizar o fluxo do processo, todos os cadastros de pessoas (exceto alunos e funcionários) do ERP TOTVS foi importado para o Sistema de Acesso. O fluxo de criação de uma visita está descrito na Figura 5.

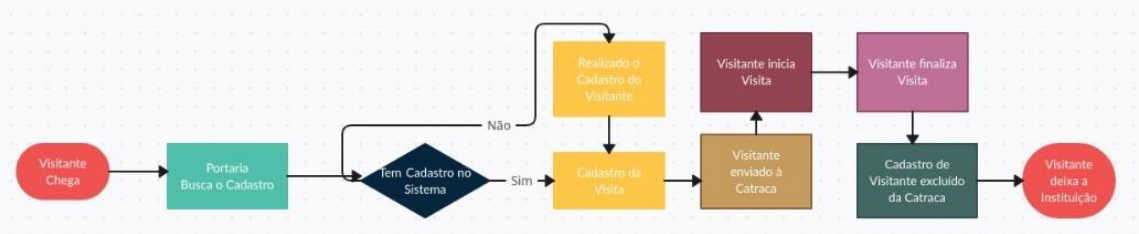


Figura 5 : Fluxo de criação de visita.

3. RESULTADOS E DISCUSSÃO

A diferença de performance no uso do reconhecimento facial em comparação à identificação por cartão de acesso ou biométrica via digital é considerável. Em relação ao cartão de acesso, a identificação biométrica facial é pelo menos 3x mais rápida, e comparando Facial x Digital, os números ficam ainda mais elásticos, chegando a uma média de 8x mais rápida. Os números do tempo estimado de acesso podem ser visualizados na Tabela 1.

Tabela 1 : Tempo estimado de acesso.

	Cartão de Acesso	**Biométrica Digital**	**Biométrica Facial**
Tempo Estimado	3s	8s	1s

Utilizar o software Gerenciador de Inners (Figura 6) descentraliza a informação. Outro problema encontrado era o controle de acesso em tempo real através de relatórios: primeiro, precisava-se, baixar (no software Gerenciador de Inners) um arquivo contendo o log dos acessos (um arquivo de texto simplesm que continha as identificações do usuarios, data e hora do acesso) e a partir dele, trabalhar a coleta de informações. A lentidão da comunicação com as catracas também era motivo de incômodo, e o próprio fabricante disponibiliza informações de limitação de taxa de transferência de dados do layout das digitais coletadas. Para integração, ainda era necessário usar um computador específico como servidor (SUPORTE TOPDATA, 2024). o que limitava o acesso as informações. As catracas funcionavam no modo chamado de “offline”, necessitando que novos cartões ou identificações biométricas fossem enviadas manualmente cada vez que coletadas.

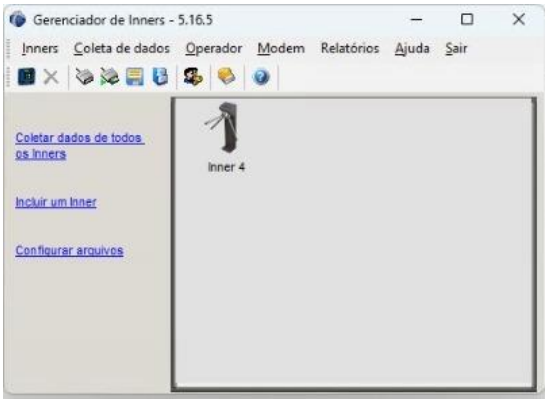


Figura 6 : Tela do Gerenciador de Inners (Catracas).

O uso de cartões de acesso (Figura 7), apesar de ter números aceitáveis em relação ao tempo estimado para liberação do acesso, traz como problemas os custos adicionais de impressão. Além dete custo fixo todos os semestres, ainda existia o problema da segurança, onde um usuário poderia ceder seu cartão de identificação para outro não autorizado. Outro problema comum nos cartões de acesso era o desgaste da impressão e por consequencia, reimpressão para segunda via, já que o mesmo era utilizado sendo inserido fisicamente em um leitor.

Figura 7 : Modelo de cartão de acesso com código de barras.

Já no caso do acesso por biometria por digital, o tempo estimado médio era muito superior até mesmo ao do cartão de acesso. Nesse modo, todas as digitais eram armazenadas no próprio equipamento e de acordo com a própria documentação das catracas (SUPORTE TOPDATA, 2024) a identificação biométrica funciona da seguinte maneira: “O usuário entra apenas com a digital, dessa forma o Inner bio irá buscar no seu banco de dado de digitais, comparando a digital inserida pelo leitor com todas as digitais cadastradas no banco de dados do Inner bio. Esse tipo de comparação é conhecida como 1 para N (muitos), é o tipo mais lento de comparação e seu tempo de resposta pode ser de 1 à 7 segundos, dependendo da quantidade de usuários cadastrados e da qualidade da digital.”.

Na ação de coletar digitais, era necessário também adquirir um leitor biométrico de digitais compatível com o software Gerenciador de Inners. O processo de coleta e envio é relativamente moroso se comparado a captura de uma foto. Ainda eram coletadas as digitais de 2 dedos diferentes, com pelo menos 90% de acurácia, conforme ilustra a Figura 8.

Figura 8 : Tela para coleta de digitais.

A instalação do dispositivo iDFace diretamente integrado à catraca (Figura 9) permite que o mesmo se comunique de forma transparente e quando há a liberação de acesso, os braços da catraca são liberados automaticamente.

Figura 9 : Dispositivo iDFace integrado à Catraca.

Para autorização de um usuários, a identificação é feita no próprio dispositivo. Quando o usuário se posiciona em frente ao identificador facial, o mesmo reconhece a pessoa e envia uma solicitação ao webservice buscando autorização para abertura da catraca. O webservice do idface busca a informação com o webservice correspondente (totvs ou acesso) e retorna para o dispositivo o status do usuário. Todas as entradas são registradas com informações como data, hora, usuário e número da catraca para emissão de relatórios.

O fluxo de funcionamento do processo de integração catracas x identificador facial x webservices pode ser visualizado na Figura 10:

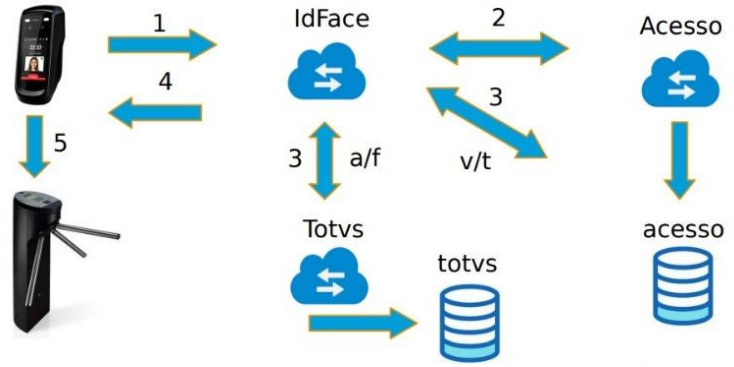


Figura 10 : Fluxo de funcionamento do processo de identificação.

Foram instaladas um total de 4 (quatro) catracas (Figura 11) com identificadores biométricos faciais na portaria do ISECENSA, para que o fluxo de acesso dos usuários em horários de maior movimento fosse atendido sem que houvessem gargalos ou filas, garantindo conforto, comodidade e segurança para todos.

Figura 11 : Catracas com Identificação Facial.

4. CONCLUSÕES

A implementação da solução de acesso via reconhecimento facial pode ser considerada um sucesso, levando em consideração todas as variáveis encontradas no ambiente escolar. A comunicação entre sistemas heterogêneos, foi resolvida com a implementação de webservices próprios, provendo informações precisas para o correto funcionamento dos dispositivos. A velocidade da identificação e autorização só é possível de ser alcançada pois a infraestrutura de rede local e servidores, com equipamentos de última geração, é gerenciada por equipe da própria instituição.

As fotos dos usuários são coletadas em ambiente controlado e com iluminação adequada, atendendo a todos os parâmetros definidos pelo fabricante do iDFace (CONTROLID, 2024). Isso garante que a quantidade de falsos-positivos seja praticamente nula.

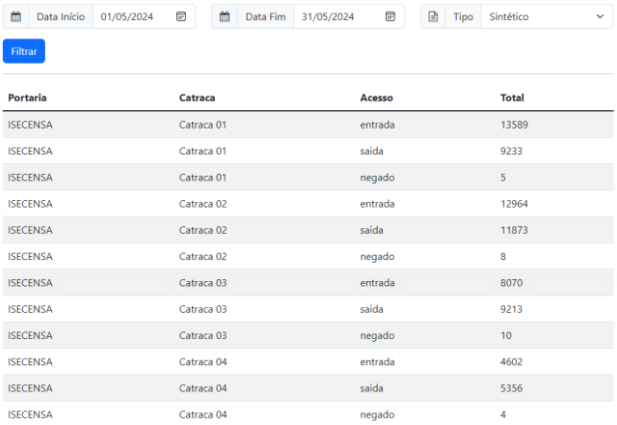
Todas as ftos são armazenadas nos sistemas correspondente: ERP TOVS para alunos e funcionários, e Sistema de Acesso para visitantes e terceirizados. Esta padronização é importante para a normalização da informação, facilitando a manutenção dos banco de dados correspondentes.

O Sistema de Acesso foi projetado para receber diferentes módulos (Figura 12) e está sob constante atualização,, buscando atender as eventuais mudanças nas regras de negócio da instituição. Controle de funcionários terceirizados, visitantes, emissão de relatórios, entre outros, estão entre as funcionalidades contempladas pelo sistema, que se tornou parte importante do dia-a-dia da instituição.

Figura 12 : Menu dos módulos contemplados até o momento no Sistema de Acesso.

A Figura 13 mostra um relatório com o recorte do mês 05/2024 (maio de dois mil e vinte quatro), onde as catracas foram usadas quase 75.000 (setenta e cinco mil) vezes, entre entradas

e saídas. O Sistema de Acesso também foi integrado ao reconhecimento facial, buscando proporcionar mais comodidade para o usuário externo que precisa visitar as instalações do ISECENSA sem que se abrisse mão da segurança, já que o mesmo deve ter seus dados cadastrados e capturada sua foto para o reconhecimento e posterior início e término da visita.


Data Início 01/05/2024 Data Fim 31/05/2024 Tipo Sintético

Filtrar

Portaria	Catraca	Acesso	Total
ISECENSA	Catraca 01	entrada	13589
ISECENSA	Catraca 01	saida	9233
ISECENSA	Catraca 01	negado	5
ISECENSA	Catraca 02	entrada	12964
ISECENSA	Catraca 02	saida	11873
ISECENSA	Catraca 02	negado	8
ISECENSA	Catraca 03	entrada	8070
ISECENSA	Catraca 03	saida	9213
ISECENSA	Catraca 03	negado	10
ISECENSA	Catraca 04	entrada	4602
ISECENSA	Catraca 04	saida	5356
ISECENSA	Catraca 04	negado	4

Figura 13 : Relatório de acesso das catracas no mês de maio / 2024.

Finalizando, é importante salientar que nenhuma regra ou sistema serão efetivos caso as pessoas responsáveis pelos processso não estejam alinhadas com as novas regras que a instituição definiu e implantou. Essa mudança comportamental é fundamental para o sucesso do projeto.

5. REFERÊNCIAS

AMER K. A.; ZEESHAN, G. A.; R, U. A; **Access Control Using Facial Recognition**. INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND

MANAGEMENT. VOLUME: 08 ISSUE: 04 | APRIL – 2024. ISSN: 2582-3930.

CHOWDHURY, M.; GAO, J.; ISLAM, R.; (2017). **Biometric Authentication Using Facial Recognition**. In: Deng, R., Weng, J., Ren, K., Yegneswaran, V. (eds) Security and Privacy in Communication Networks. SecureComm 2016. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 198. Springer, Cham. https://doi.org/10.1007/978-3-319-59608-2_16

CONTROLID. **Controle de Acesso iDFace. Control ID**. Disponível em <https://www.controlid.com.br/controle-de-acesso/idface/>. Acesso em 01 ago 2024.

EASY INNER. **SDK EasyInner (Catracas e Coletores)**. Disponível em <https://suporte.topdata.com.br/suporte/sdk-easyinner/>. Acesso em 30 jul 2024.

GALHARDO, A. T.; **Sistemas Eletrônicos de Controle de Acesso**. 46f. Monografia (Bachalerado em Engenharia Elétrica) - Universidade São Francisco, São Paulo, 2011.

ITPRO. **The pros and cons of facial recognition technology**. Disponível em <https://www.itpro.com/security/privacy/356882/the-pros-and-cons-of-facial-recognition-technology>. Acesso em 05 ago 2024.

MEDURI, R.K.K. (2019). **Webservice Security**. In: Mohanty, H., Pattnaik, P. (eds) Webservices. Springer, Singapore. https://doi.org/10.1007/978-981-13-3224-1_6

MISSINI, E; LAJÇI, U; (2022) **Biometric Authentication**. Department of Computer and Software Engineering, University of Prishtina Pristina, Kosovo. 2022.

MOHANTHY, H; PATTNAIK, P. K.; (2019) **Webservices Engineering: Theory and Practice**. 1st ed. Springer Singapore. ISBN: 978-981-13-3223-4. 196p.

PINHEIRO, J. M.; **Biometria nos Sistemas Computacionais**. 1ª Edição. Ciência Moderna, 2008. ISBN: 978-85-7393-738-1

SOUZA, M. B.; **Controle de Acesso: Conceitos, Tecnologias e Benefícios**. 2010. Editora Sicurezza.

SUPORTE TOPDATA. **Manuais catraca Revolution**. Disponível em <https://suporte.topdata.com.br/categorias/revolution-manuais/>. Acesso em 30 jul 2024.

TOPDATA. **Catracas Eletrônicas para controle de acesso**. Disponível em <https://www.topdata.com.br/catracas/>. Acesso em 23 jul 2024.

TOTVS. **Melhor sistema de Gestão Educacional é TOTVS**. Disponível em <https://www.totvs.com/educacional/>. Acesso em 20 jul 2024.