**UNIVERSIDADE NOVE DE JULHO – UNINOVE**

**CURSO DE CIÊNCIA DA COMPUTAÇÃO**



***Segurança da informação na FaceRec***

**SÃO PAULO**

**2019**

**Segurança da informação na FaceRec**

**André Cardoso Aragão RA – 918119401**

Trabalho apresentado ao curso de Ciência da Computação da Universidade Nove de Julho, como parte dos requisitos para a obtenção do Grau de Cientista da Computação.

Orientador: Prof. Ms. Norberto dos Santos

Unidade: Campus Memorial

Curso: Ciência da Computação

Período: Matutino

São Paulo

2019

**FOLHA DE APROVAÇÃO**

**André Cardoso Aragão RA – 918119401**

**Segurança da informação na FaceRec**

Trabalho de conclusão aprovado como requisito parcial para a obtenção do grau de Cientista da computação, do curso de Ciência da Computação, da Universidade Nove de Julho, pelo professor orientador abaixo mencionado.

São Paulo, 01 de dezembro de 2019

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Prof. Ms. Norberto dos Santos

**RESUMO**

Esse projeto é uma maneira de demonstrar a importância da segurança da informação. Através de regras e métodos existentes no mercado, será demonstrado o que está em risco quando a segurança da informação não tem o devido cuidado necessário dentro de uma empresa que busca o sucesso e reconhecimento. Levando em conta o estudo dessas regras e metodologias, fica claro que o sucesso de uma empresa depende totalmente de como lidam com suas informações e as informações dos clientes. Por fim, entende-se que a segurança da informação é uma das áreas onde deve-se ter o maior cuidado dentro de uma empresa e setor de TI.

Palavras-chaves: Segurança; Informação; Riscos.

**ABSTRACT**

This project is a way to show the importance of the information security. Through rules and methods that exist in the market, will be shown what is in risk when the information security doesn’t had the care that is needed inside a company that seeks success and acknowledgment. Taking into account the studying of these rules and methodologies, stay clear that the success of a company totally depends of how they deal with their information and the customers information. By the end, it’s known that information security is one of the areas where must have to be carefull inside a company and in the IT sector.

Keywords: Security, Information, Risks.

**LISTA DE FIGURAS**

**Figura 1** – Data Center da FaceRec…………………………………………………………

**Figura 2** – Sala de Segurança da FaceRec…………………………………………………

**LISTA DE TABELAS**

**Tabela 1** – Matriz GUT……………………………………………………………………...

**LISTA DE ABREVIATURAS E SIGLAS**

**CFTV -** *Closed-Circuit Television*

**ERP -** *Enterprise Resource Planning*

**PSI -** Política de Segurança da Informação

**RH -** Recursos Humanos

**GUT -** Gravidade Urgência Tendência

**SUMÁRIO**

[**1. INTRODUÇÃO**](#_r6fg3ubr5il6)**………………………………………………………………………….... 9**

[1.1 OBJETIVOS](#_rykm6vh65lem)………………………………………………………………………………. 9

[**2. A EMPRESA**](#_dgacn743m99)**…………………………………………………………………………....... 10**

[2.1 ESTRUTURA](#_73c5yytx9ioq)………………………………………………………………………...…. 10

[2.2 ROTINA ATUAL](#_mgvjqb94ux49)……………………………………………………………………....... 10

[**3. ANÁLISE DE RISCO - NOVO SOFTWARE**](#_l3r2hptibvom)**…………………………………………. 12**

[3.1 VULNERABILIDADES](#_3y723or2opud) 12

[3.2 AMEAÇAS](#_w6mbgofq28cj)…………………………………………………………………………….... 12

[3.3 IMPACTOS](#_m2z8wtt742wj)…………………………………………………………………………….... 12

[3.4 SOLUÇÕES](#_ffgfu2joxuly)……………………………………………………………………………... 12

[**4. POLÍTICA DE SEGURANÇA DE ENTRADA E SAÍDA**](#_vhk6krohl0f2)**……………………………. 14**

[4.1 ACESSO AO PRÉDIO](#_cqfea3zbv8o7)………………………………………………………………….. 14

[4.2 ACESSO AO DATA CENTER](#_jak3blsmk9p)………………………………………………………….. 14

[4.2.1 ACESSO AO LOCAL](#_dntv54m0kc1q)…………………………………………………………………. 14

[4.2.2 ACESSO AO BANCO DE DADOS](#_dxz973dryx10)…………………………………………………... 15

[**5. POLÍTICA DE VIGILÂNCIA**](#_bdl4riysudzd)**……………………………………………………………………. 16**

[5.1 ACESSO ÀS INFORMAÇÕES DE SEGURANÇA](#_f340my5lbq77)…………………………………………. 16

[**6. CLASSIFICAÇÃO E CICLO DE VIDA DAS INFORMAÇÕES**](#_7h7r6dw3ev4)**…………………………….. 17**

[6.1 CLASSIFICAÇÃO E CUSTODIANTES DAS INFORMAÇÕES](#_gdtxjfg27aoa)………………………….... 17

[6.1.1 INFORMAÇÕES DOS CLIENTES](#_qx06mt6b91ca) ………………………………………………………....17

[6.1.2 INFORMAÇÕES DOS USUÁRIOS](#_9ykrku5l16b) ………………………………………………………...17

[6.1.3 INFORMAÇÕES DOS SOFTWARES](#_c0p9uly4edmo) ……………………………………………………..17

[6.2 TRANSPORTE DAS INFORMAÇÕES](#_vh5v5n71x36) ……………………………………………………….17

[6.3 DESCARTE DAS INFORMAÇÕES](#_hfczso68ft4o) …………………………………………………………..18

[**7. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**](#_loprf7i109dj) **…………………………………………...19**

[7.1 ACESSO À INTERNET E SEU USO](#_t1vtdgpk8mc6) ………………………………………………………....19

[7.1.1 POLÍTICA DE USO DAS FERRAMENTAS DA EMPRESA](#_fyh4n2fzk4lk) ……………………………..19

[7.2 POLÍTICA DE DISPOSITIVOS ELETRÔNICOS](#_v6arr7isz13r) …………………………………………....19

[7.3 PUNIÇÃO PARA VIOLAÇÃO DE ALGUMA POLÍTICA](#_ovw25a4owdad) …………………………………….20

# 1. INTRODUÇÃO

Esse projeto irá abordar diversas áreas da Segurança da informação e como aplicá-los no dia-a-dia de uma grande empresa, com muitos funcionários e infraestrutura de ponta. Serão mostrados diversos métodos para cuidar do que é mais importante nessa empresa: as informações, pois apenas com o bom uso das informações uma empresa poderá prosperar.

Cada dia que passa há mais informações para serem guardadas, algumas acabam exigindo um cuidado extremo, caso essas informações sejam acessadas por pessoas não autorizadas, pode causar um dano irreparável na empresa.

Nos capítulos a seguir será mostrado como cuidar da segurança física e lógica das informações e como fazer isso da melhor maneira, com melhor custo e qualidade máxima, minimizando todos os riscos possíveis.

## 1.1 OBJETIVOS

O principal objetivo do projeto é demonstrar a complexidade e a importância dos cuidados com todos os dados e informações em uma empresa nos dias atuais, devido aos grandes perigos que existem atualmente.

Junto com esse objetivo vem a missão de mostrar uma maneira de cuidar de tudo isso e incentivar a nunca deixar de lado esses cuidados e buscar ao máximo otimizar a segurança para que nada indesejado aconteça.

# 2. A EMPRESA

A empresa fictícia que será abordada é a “FaceRec”, uma empresa focada em desenvolver programas de reconhecimento facial, ela desenvolve softwares para outras empresas do mundo todo, seja para empresas de produtos eletrônicos ou também programas para serem utilizados como sistema de segurança para entrada e saída.

## 2.1 ESTRUTURA

A sede da empresa é constituído pelos seguintes itens:

* + Um total de 800 computadores separados em quatro andares diferentes;
  + 105 Impressoras departamentais;
  + Há um controle de entrada e saída na entrada principal e no estacionamento;
  + Vigilância total em CFTV;
  + Data Center para informações da empresa e também dos clientes.

## 2.2 ROTINA ATUAL

Atualmente a empresa trabalha na implementação de uma opção no software principal do sistema de entrada e saída, a opção de bloquear acesso está muito lenta atualmente e estão trabalhando nisso.

Diariamente a equipe de RH está entrevistando pessoas para entrarem no grupo de marketing da empresa, isso está em uma das principais tarefas atualmente, pois o índice de novos clientes está diminuindo drasticamente.

A equipe de teste está vendo se há algum problema no software mais novo da empresa, que será entregue para duas empresas no final do mês, que está sendo a prioridade máxima, pois se atrasar haverá multa contratual. Esse evento tem uma análise de risco que será descrita em breve.

Os diretores têm uma reunião com os fornecedores final do mês e devem começar a planejar a apresentação o mais rápido possível.

A tesouraria deve entregar o relatório financeiro no começo do próximo mês, junto com uma previsão futura dos lucros.

Abaixo(Tabela 1) está a matriz GUT para essa rotina atual, onde mostra(de 1 a 5) a gravidade, urgência e tendência do problema. Quanto maior o número da coluna prioridade, mais rápido essa tarefa deve ser concluída.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tarefas** | **Gravidade** | **Urgência** | **Tendência** | **Prioridade** |
| Contratação em Marketing | 3 | 5 | 5 | 13 |
| Implementação Software Entrada/Saída | 3 | 4 | 4 | 11 |
| Teste novo Software | 4 | 5 | 5 | 14 |
| Reunião Importante - Planejamento | 5 | 3 | 4 | 12 |
| Relatório Financeiro | 2 | 2 | 3 | 7 |

**TABELA 1 – Matriz GUT**

# 3. ANÁLISE DE RISCO - NOVO SOFTWARE

Esse novo software que está em teste, será enviado futuramente para duas empresas gigantes no mercado, por isso foi de extrema importância fazer uma análise de risco desse projeto, pois é totalmente confidencial entre essas duas empresas parceiras.

De acordo com Sêmola (2014 p.41), "podemos definir segurança da informação como uma área de conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade."

Com essa análise de risco das informações do projeto foi possível minimizar as possibilidades de alguma informação ser vazada.

## 3.1 VULNERABILIDADES

Lista de vulnerabilidades em relação às informações do projeto:

* + Acesso de muitas pessoas no ambiente de desenvolvimento;
  + Comunicação via e-mail ou mensagem de texto pode ser um risco;
  + Alguém poderia acabar abandonando o projeto e levando com ele informações importantes;
  + Desenvolvedores que levam trabalho para finalizar em casa.

## 3.2 AMEAÇAS

A grande ameaça que existe é se alguma informação do projeto for vazada, por causa de contrato a “FaceRec” terá que arcar com uma multa em dinheiro, com um valor muito alto. Além disso a empresa ficaria com a reputação comprometida.

## 3.3 IMPACTOS

Caso aconteça algo de errado, a “FaceRec” poderá encontrar dificuldade para encontrar novos clientes grandes, devido a esse deslize com a segurança do projeto e a reputação abalada.

## 3.4 SOLUÇÕES

Algumas soluções encontradas e que foram aplicadas:

* + Limitar quem acessa a área de desenvolvimento movendo toda a equipe para um só andar, onde só eles devem ter acesso livre a todo momento sem autorização;
  + Segurança na porta da sala verificando a identidade de quem entra e sai;
  + Todas as dúvidas e relatórios serão falados pessoalmente aos gerentes do projeto;
  + Todos trabalhando no projeto assinaram um contrato de confidencialidade;
  + Nenhum desenvolvedor deve levar esse trabalho para casa.

# 4. POLÍTICA DE SEGURANÇA DE ENTRADA E SAÍDA

Na “FaceRec” há um padrão documentado de todos os passos que as pessoas devem seguir para entrar no prédio da empresa, há documentos diferentes com passos diferentes para quem tem acesso ao Data Center. todos esses documentos são passados para os funcionários e os que há necessidade, são treinados por uma dupla que cuida da segurança física do prédio, para executar tudo de maneira correta.

Todos os procedimentos abaixo são devidamente documentados.

## 4.1 ACESSO AO PRÉDIO

Esse é o procedimento padrão que acontece tanto na entrada pelo estacionamento como na entrada principal: cada funcionário possui um crachá que é também um controle eletrônico. Esse crachá é intransferível como diz no documento. O Funcionário deve utilizar seu crachá para passar por uma catraca eletrônica e logo após passar por um reconhecimento facial, feito por um software da própria empresa, desse jeito os funcionários têm acesso ao prédio.

Pessoas comuns o procedimento é mais simples: eles devem ir na recepção contar a razão de estar querendo entrar no local, caso seja autorizada a entrada, ele receberá um crachá temporário, e ao passar pela catraca, será acompanhado por um segurança até onde a pessoa deve ir, isso é para garantir que a pessoa não vá a algum lugar que não é permitido.

## 4.2 ACESSO AO DATA CENTER

## 4.2.1 ACESSO AO LOCAL

Há poucas pessoas que têm acesso ao data center, duas delas são os dois seguranças que abrem e fecham o local todo dia, eles são treinados para ir até o local com as chaves, entrar, checar se todos saíram do local, apagar as luzes, sair e trancar as portas, as portas utilizam uma chave física e uma leitura facial. Além dos guardas, há duas equipes que têm acesso ao local diariamente, a equipe de manutenção e de limpeza, as duas equipes quando estão no local devem a todo momento estar sob vigilância não só pelo sistema de câmeras, mas também por seguranças.

Além desses três grupos de pessoas, podem haver visitantes, que possuem autorização de diretores, mesmo com essa autorização, todos os visitantes também são monitorados.

## 4.2.2 ACESSO AO BANCO DE DADOS

Para definir quem pode acessar o banco de dados, há os diretores do setor de desenvolvimento, eles decidem quem pode acessar e quando. Toda vez que alguém acessar o banco de dados deve possuir autorização desses diretores.

****

**FIGURA 1 – Data Center da FaceRec**

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 5. POLÍTICA DE VIGILÂNCIA

Na “FaceRec” há uma sala onde há uma pequena equipe de segurança composta por três seguranças, contratada para vigiar as câmeras do sistema CFTV.

## 5.1 ACESSO ÀS INFORMAÇÕES DE SEGURANÇA

Quem tem acesso às câmeras de vigilância são os funcionários de segurança, mas caso exista alguma suspeita, os diretores da empresa podem solicitar verificação das imagens ou fazer um pedido especial para a equipe executar essa ação.

****

**FIGURA 2 – Sala de Segurança da FaceRec**

# 

# 

# 

# 

# 

# 

# 

# 

# 6. CLASSIFICAÇÃO E CICLO DE VIDA DAS INFORMAÇÕES

A “FaceRec” tem total cuidado e preza pela privacidade dos usuários e clientes, para isso há diferentes níveis de acesso às informações, tentando minimizar qualquer acesso indesejável, apenas quem precisa acessar essas informações podem ter acesso.

## 6.1 CLASSIFICAÇÃO E CUSTODIANTES DAS INFORMAÇÕES

## 6.1.1 INFORMAÇÕES DOS CLIENTES

As informações de quem são nossos clientes e o que é pedido por eles, tem um nível de confidencialidade baixo a menos que eles peçam total sigilo, como pediram no nosso novo software que está em desenvolvimento.

Caso o cliente não deseja que o projeto seja secreto, todos da equipe de desenvolvimento tem total conhecimento para quem eles estão fazendo o trabalho e qual será a função do produto. Caso não seja especificado pelo cliente, a empresa pode usar o nome para o portfólio da “FaceRec”.

## 6.1.2 INFORMAÇÕES DOS USUÁRIOS

As informações dos usuários do software, como os rostos do reconhecimento facial e dados pessoais, são altamente sigilosas, e só é permitido o acesso por solicitação da legislação, tudo isso para garantir que a privacidade dos usuários seja a mais confiável possível, a informação fica disponível para ninguém dentro da “FaceRec”.

## 6.1.3 INFORMAÇÕES DOS SOFTWARES

Os desenvolvedores sênior são os únicos que podem aplicar qualquer mudança no código dos softwares, e a permissão para essas mudanças é concedida pelos diretores da área de desenvolvimento, isso ocorre para manter a integridade do software, fazendo apenas mudanças totalmente necessárias e deixar todos cientes de cada mudança.

## 6.2 TRANSPORTE DAS INFORMAÇÕES

Para garantir autenticidade de todas as informações, quando é necessário o transporte dessas informações, seja mudar de servidores, compartilhamento de código entre desenvolvedores, documentos entre as diretorias, as informações sempre são criptografadas para que só a pessoa que está recebendo e enviando tenha acesso e controle sobre a informação.

## 6.3 DESCARTE DAS INFORMAÇÕES

Quando algum cliente deixa de utilizar os serviços da “FaceRec” e rompe o contrato, as informações do software, do cliente e dos usuários ficam armazenadas por três meses para o caso do cliente retornar e buscar um novo contrato.

Após os três meses todas as informações dos usuários são apagadas, as informações do software e do cliente são gravadas em fitas para serem retiradas dos servidores, para evitar uso de espaço desnecessário.

# 7. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Na “FaceRec” todos os funcionários assinam um termo onde estão sujeitos à todas as regras contidas na PSI da empresa, quem não cumprir essas regras relacionadas a segurança da informação está passível a punição, as regras podem variar dependendo do cargo do funcionário, mas todos contêm diretrizes básicas para a segurança de todos na empresa.

## 7.1 ACESSO À INTERNET E SEU USO

No ambiente da empresa, todos têm acesso à rede da empresa através de WiFi e por meio de cabos. Para execução de tarefas todos os dispositivos devem estar conectados via cabo, conectados na rede da empresa por meio de um login.

O login deve sempre ser feito por quem está acessando a internet, e tudo que a pessoa acessar fica armazenado nos servidores, para caso haja alguma suspeita de um acesso de conteúdo que não é necessário para o trabalho fique fácil encontrar os registros.

## 7.1.1 POLÍTICA DE USO DAS FERRAMENTAS DA EMPRESA

Para utilizar as ferramentas da empresa, sempre é necessário a identificação do usuário através do login, e é proibido qualquer um utilizar as ferramentas com o registro de outra pessoa, essa regra é a que tem uma das punições mais severas caso aconteça o descumprimento por parte de algum funcionário.

Se encaixa nessa regra tanto ferramentas virtuais, como programas do computador da empresa, e também ferramentas físicas como as diversas impressoras da empresa.

## 7.2 POLÍTICA DE DISPOSITIVOS ELETRÔNICOS

Para todos os funcionários que precisam utilizar algum dispositivo eletrônico além dos computadores da empresa, seja celular, notebook ou tablet, esses dispositivos são cedidos pela empresa e são devidamente adequados para o uso restrito das ferramentas necessárias pelo usuário.

É estritamente proibido executar tarefas do trabalho em dispositivos pessoais, apenas é permitido executar tarefas em dispositivos cedidos pela empresa.

## 7.3 PUNIÇÃO PARA VIOLAÇÃO DE ALGUMA POLÍTICA

Caso alguém descumpra algum dos termos da PSI, sua infração será avaliada pelo diretor do departamento em que trabalha e após a avaliação o diretor irá aplicar a punição, essa punição pode variar de perder alguns dias de trabalho, ser movido de função, ou até o seu desligamento da empresa em casos graves.

**CONCLUSÃO**

Nesse projeto, abordamos as diversas áreas da segurança da informação, atingindo o objetivo de mostrar a complexidade e importância do cuidado com as informações em uma empresa, além de incentivar a ter cada vez mais cuidado com a segurança da informação no dia-a-dia.

Desenvolver esse projeto foi de extrema importância, pois mesmo achando que entendia os cuidados que deve-se ter com a segurança da informação, através desse projeto foi possível descobrir diversos outros tópicos que também são necessários ter extrema cautela, é um assunto muito complexo e delicado e a cada dia que passa o cuidado deve aumentar devido ao aumento de ameaças à segurança da informação dia após dia.

Através de todo esse estudo, conclui-se que a cada dia que passa o cuidado com as informações deve aumentar, pois todas as empresas buscam o lucro, apenas com o cuidado que as informações precisam, é possível atingir o sucesso em uma empresa.

**REFERÊNCIA BIBLIOGRÁFICA**

ERP – O que é e como funciona. Disponível em: <<https://www.sispro.com.br/blog/erp/erp-o-que-e-e-como-funciona/>>. Acesso em: 22 de out. de 2019.

OTÁVIO, Luis. RECONHECIMENTO FACIAL: COMO FUNCIONA. Disponível em: <<https://usemobile.com.br/reconhecimento-facial-como-funciona/>>. Acesso em 22/10/2019.

MOREIRA, Esdras. O que é a Política de Segurança da Informação (PSI)?. Disponível em: <<https://introduceti.com.br/blog/o-que-e-a-politica-de-seguranca-da-informacao-psi/>>. Acesso em 22/10/2019

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. Política de Segurança da Informação: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. Gerenciamento de Serviços de TI na Prática: uma abordagem com base na ITIL. São Paulo: Novatec, 2007.

SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva. Rio de Janeiro: Elsevier, 2003.

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício de. Segurança de Redes em Ambientes Cooperativos. São Paulo: Berkeley, 2002.

WADLOW, Thomas A. Segurança de Redes: projeto e gerenciamento de redes seguras. Rio de Janeiro: Campus, 2001