UNIVERSIDADE NOVE DE JULHO – UNINOVE
CURSO DE TECNOLOGIA EM REDES DE COMPUTADORES


# Projeto de implantação de segurança da informação

## Grupo Droga Rias LTDA

SÃO PAULO
2020

# Projeto de implantação de segurança da informação
# Grupo Droga Rias LTDA


Fernando Seabra Anjos RA – 2220201535

Michel Augusto Debia Vieira Coelo RA – 920122024

Thiago Vieira Matias dos Santos RA – 420114556

Vinicius Corrêa Albuquerque RA – 919209291


Trabalho apresentado ao curso de Tecnologia em Redes de Computadores da Universidade Nove de Julho, como parte dos requisitos para a obtenção do Grau Superior.

Orientador: Fabio de Jesus Souza

Unidade: Campus Vergueiro

Curso: Tecnologia em Redes de Computadores

Período: Manhã

São Paulo
2020

FOLHA DE APROVAÇÃO


Fernando Seabra Anjos RA – 2220201535

Michel Augusto Debia Vieira Coelo RA – 920122024

Thiago Vieira Matias dos Santos RA – 420114556

Vinicius Corrêa Albuquerque RA – 919209291


# Projeto de implantação de segurança da informação
# Grupo Droga Rias LTDA

Trabalho de conclusão aprovado como requisito parcial para a obtenção do grau superior, do curso de Tecnologia em redes, da Universidade Nove de Julho, pelo professor orientador abaixo mencionado.

São Paulo, 18 de Novembro 2020

_____

Prof. Fabio de Jesus Souza

**RESUMO**

O projeto visa aplicar a segurança da informação para o Grupo Droga Rias LTDA, que atualmente teve algumas informações de clientes coletadas de sua base de dados devido as vulnerabilidades e falhas na segurança.

Com isso foi solicitado a nossa empresa, que realizasse uma análise de risco, e ajustasse os processos para mitigar as falhas.

O Grupo Droga Rias LTDA, está no mercado à 10 anos, e teve sua rede ampliada principalmente nos últimos anos devido à grande demanda de medicamentos.

Com esse crescimento, não foi estudado as possíveis falhas de segurança que poderiam acontecer com a rede toda da marca.

Este projeto irá abranger toda a parte de segurança da informação tanto lógica quanto física.

**ABSTRACT**

The project aims to apply information security to Grupo Droga Rias LTDA, which currently had some customer information collected from its database due to security vulnerabilities and flaws.

As a result, our company was asked to carry out a risk analysis and adjust the processes to mitigate failures.

Grupo Droga Rias LTDA, is in the market at the age of 10, and its network has expanded mainly in recent years due to the great demand for medicines.

With this growth, it was not studied as possible security flaws that could happen with the entire brand network.

This project will cover all information security as well as physical logic.

**Keywords:** AWS, RSICO, SEVENSHOP, TREINAMENTO, ISO

**LISTA DE FIGURAS**

FIGURA 1 – Faixada de uma das lojas Droga Rias

FIGURA 2 – Logotipo servidor DynamoDB

FIGURA 3 – Modelo ThinClient

FIGURA 4 – Especificações técnicas Thin Client

FIGURA 5 – Amazon WorkSpaces

FIGURA 6 – Software gestão farmacêutico

**LISTA DE TABELAS**

TABELA 1 -Tabela de custos com equipamentos e softwares

TABELA 2 – Matriz de Setup

**SUMÁRIO**

1.0 INTRODUÇÃO.....8

1.1 OBJETIVOS.....9

2.0 CLASSIFICAÇÃO DA INFORMAÇÃO.....9

3.0 ANÀLISE DE RISCO.....10

4.0 MEDIDAS ADOTADAS.....11

5.0 EQUIPAMENTOS E SERVIÇOS.....12

5.1 SERVIDOR DE BANCO DE DADOS E APLICAÇÕES 12.....12

5.2 ESTAÇÔES DE TRABALHO.....13

5.3 SOFTWARE PARA GESTÃO.....14

6.0 TREINAMENTOS DE USUÁRIOS.....15

7.0 DIMINUIÇÃO DE RISCO .....17

7.1 AMBIENTE EM NUVEM AWS ESTAÇÕES E SERVIDORES.....17

7.2 AJUSTE DE CONCESSÃO DE ACESSO.....17

7.3 TREINAMENTO E CONCIENTIZAÇÃO.....17

8.0 CUSTO BENEFÍCIO.....18

9.0 PUNIÇÕES.....19

10.0 AVAL EQUIPE TECNICA.....20

CONCLUSÃO

REFERÊNCIAS

## 1.0 INTRODUÇÃO

O grupo Droga Rias está no mercado a 10 anos, distribuindo medicamentes para toda a população da Zona Sul de São Paulo.


Figura 1 – Faixada de uma das lojas Droga Rias

O grupo cresceu suas receitas nos últimos anos devido à alta demanda de medicamentos, o grupo que antes continha somente 2 lojas, hoje possuem 100 lojas espalhadas na Zona sul de São Paulo.

Vamos auxiliar o pessoal da Droga Rias a implementar a segurança da informação em suas lojas.

Usaremos a PSI para aplicar conforme procedimentos, que tratam de controles tanto físicos quanto lógicos, testes e verificações de controles internos e demais atividades inerentes ao varejo de medicamentos.

Essa política abrange todos os empregados, conselheiros e dirigentes das lojas, e ainda o estagiários, aprendizes, fornecedores e prestadores de serviço do Grupo Droga Rias LTDA que possuem acesso a equipamentos computacionais e quaisquer ambientes que necessitem de Login, e é obrigação destes manterem-se atualizados a este termo, procedimentos e normas da empresa.

## 1.1OBJETIVOS

Este documento visa instituir a segurança da informação com base nas análises de risco do ramo farmacêutico e do perfil do negócio, além de apresentar os mecanismos de segurança utilizados para garantir a confiabilidade, integridade e disponibilidade da informação. A política trata conscientizar os colaboradores e as partes interessadas que possam ter acesso às informações no tratamento desenvolvido pelo Grupo Droga Rias LTDA, que compõe um comportamento ético e profissional aos usuários da rede de modo a trazer ao conhecimento da coletividade a forma de lidar adequadamente com os recursos de informática.

## 2.0 CLASSIFICAÇÃO DA INFORMAÇÃO

De acordo com a **ISO 270001**, a classificação da informação deve ser feita por conta própria, desta forma foi verificado com a direção para estabelecer critérios em relação a confidencialidade dos dados no Grupo Droga Rias LTDA, conforme as definições a seguir para fins dessa política:

I – Restrita: é toda informação ao qual somente o usuário, empregado ou gestor do Grupo Droga Rias LTDA, por meio de seu Login e senha, possui acesso. A divulgação não autorizada dessa informação poderá causar danos financeiros e/ou comprometer estratégias do negócio.

II – Confidencial: Toda informação gerada por fontes internas ou externas às drogarias, das quais se faz necessário o sigilo por obrigação legal. A divulgação não autorizada desta informação poderá causar problemas jurídicos ao grupo.

III – Interna: Toda informação de interesse operacional das drogarias.

IV – Pública: São as informações que podem ser acessadas por todos, sem prejuízo legal, financeiro ou estratégico.

## 3.0 ANÀLISE DE RISCO

O processo de gerenciamento de riscos, como todo procedimento de tomada de decisões, começa com a identificação e a análise de um problema. No caso do gerenciamento de riscos, o problema consiste, primeiramente, em se conhecer e analisar os riscos de perdas acidentais que ameaçam a organização. A identificação de riscos e perigos consiste em uma importante responsabilidade do grupo Droga Rias LTDA.

É o processo por meio do qual as situações de risco são analisadas de forma contínua e sistemática.

Alguns dos riscos mais comuns em uma drogaria são:

- Queda de energia;
- Software de gestão parar de funcionar;
- Queda de internet;
- Queda da Anvisa (Para enviar o controle dos medicamentos controlados);
- Funcionários com acesso a relatórios gerenciais;
- SAT com a luz Fail acessa;
- Falhas no ThinClient (computador);

A seguir temos a tabela de matriz de setup dos riscos mais comuns contidos no levantamento do cliente Droga Rias.

| Item | Disponibilidade | Integridade | Impacto | Probabilidade |
|---|---|---|---|---|
| Queda de energia | **Alto** | **Alto** | **Alto** | **Médio** |
| Software de gestão parar de funcionar; | **Alto** | **Alto** | **Alto** | **Baixo** |
| Queda de internet | **Alto** | **Alto** | **Alto** | **Médio** |
| Queda da Anvisa (Para enviar o controle dos medicamentos controlados) | **Alto** | **Alto** | **Alto** | **Baixo** |
| Funcionários com acesso a relatórios gerenciais | **Alto** | **Médio** | **Baixo** | **Médio** |
| SAT com a luz Fail acessa | **Alto** | **Médio** | **Alto** | **Médio** |
| Falhas no ThinClient (computador) | **Alto** | **Baixo** | **Baixo** | **Médio** |

TABELA - Matriz de setup para análise de risco

## 4.0 MEDIDAS ADOTADAS

Medidas adotadas para a prevenção dos riscos citados anteriormente na mesma ordem:

- Adquirimos nobreaks para estar prontos caso uma queda de energia ocorra;
- Contamos com Suporte técnico 24h caso qualquer problema relacionado a softwares ocorra.
- As drogarias do Grupo Droga Rias LTDA contam com uma operadora de internet de contingencia caso a primeira apresente instabilidade ou queda.
- Caso ocorra problemas para o envio dos lotes dos medicamentos controlados as dúvidas devem ser sanadas diretamente com a Anvisa pelo número 0800 642 9782.
- O SevenShop conta com um excelente esquema de acesso por senhas, por meio dele cada colaborador só tem acesso ao necessário para a execução de suas funções;
- Caso o SAT esteja na garantia solicitar a troca do equipamento, caso não esteja na garantia adquirir um equipamento novo, lembrando que a rede Droga Rias LTDA conta com um SAT de contingência em todas as suas lojas.
- Contamos com um ThinClient de contingencia, com todos os sistemas já configurados, em cada loja, o ThinClient que apresentar falhas será encaminhado para o suporte técnico.

O grupo Droga Rias LTDA preza pela segurança dos dados dos colaboradores, clientes e fornecedores cadastrados em seu sistema, todas as medidas foram adotadas para garantir tranquilidade e segurança na prevenção de riscos.

## 5.0 EQUIPAMENTOS E SERVIÇOS

Hoje o Grupo Droga Rias LTDA utilizam computadores em cada uma das suas filiais, além de cada uma das filiais conter um servidor de banco de dados próprio, aonde é armazenado todos os dados cadastrais dos clientes e dados financeiros da unidade.

Em análise foi considerando que esse tipo de armazenagem de dados local não é segura, pois o cliente não contém nenhum backup das informações, além de facilitar o roubo de dados sigilosos.

Com isso estamos migrando toda a parte de servidores e desktop para a plataforma AWS.

## 5.1 SERVIDOR DE BANCO DE DADOS E APLICAÇÕES

Para o servidor de banco de dados e aplicação, utilizaremos o Amazon DynamoDB, este teremos uma total disponibilidade dos dados, além de backup provisionado pelo próprio ambiente da AWS.


Figura 2 - Logotipo servidor DynamoDB

No serviço também temos disponíveis o serviço de replicação do servidor sem custo adicional, com isso deixamos o ambiente redundante e com alta disponibilidade.

## 5.2 ESTAÇÔES DE TRABALHO

As estações de trabalho das unidades estavam com seu hardware defasado, com isso decidimos instalar em todas as unidades os equipamentos ThinClient, para acessar as estações em nuvem.

Figura 3 – Modelo ThinClient

Esse equipamento tem as seguintes configurações.

**Especificações**

| | |
|---|---|
| Processador | ARM A53 QuadCore 2.0GHz |
| Memória | 512MB - RAM / 4GB - ROM |
| S.O. embarcado | Linux |
| Resolução de vídeo VGA / HDMI | 800*600/1024*768/1366*768 / 1440*900/1280*1024/1600*900/1920*1080 (MAX) |
| Dimensões | 10,7cm x 10,7cm x 2,8cm |
| Peso | 200g |
| Protocolo | RDP 8.1 |
| Consumo de energia | Estática menor que 5W / Potência máxima menor que 7.5W |

Figura 4 – Especificações técnicas Thin Client

O serviço escolhido para comportar todo o ambiente desktop do projeto é o Amazon WorkSpaces, com ele temos total autonomia para criar ou deletar estações de trabalho que não sejam mais necessárias, além de termos o serviço de segurança e backup disponíveis na Amazon, tudo isso sendo acessado dos equipamentos ThinClient.


Figura 5 – Amazon WorkSpaces

## 5.3 SOFTWARE PARA GESTÃO

Nosso cliente utilizava um software próprio, que já estava defasado com relação a outros que temos no mercado, com isso implantaremos o Sofware de gestão SevenShop que é um software de gestão para varejo.


FIGURA 6 – Software gestão farmaceutico

Nele o cliente terá todos os módulos necessários para gestão do negócio disponível em um só sistema, este software será instalado em nossos servidores do ambiente AWS, protegido assim pela mais alta segurança e contendo backups de segurança oferecidos pela Amazon.

Cada estação virtual terá acesso ao módulo da SeveShop, com seus dados sendo totalmente armazenados e centralizados em nosso servidor em nuvem de banco e aplicação Amazon DynamoDB

Valores dos custos com Softwares e hardwares

| Produto | Descrição | Valor unitário | Total | Observações |
|---|---|---|---|---|
| Servidores em nuvem (AWS) | Dynamo | 2.000R$DB | 2.000 | Mensais |
| Máquinas | ThinClient | 130,00 R$ | 13.000 | 130 Equipamentos |
| Software desktop(AWS) | Amazon Work Space | 100 R$ | 13.000 | AWS |
| Software adminsitração | Seven Shop | 1.000 | 1.000 | Mensais |
| TOTAL | | | 29.000 | |

Tabela 1 -Tabela de custos com equipamentos e softwares

## 6.0 TREINAMENTOS DE USUÁRIOS

O treinamento de usuários consiste em conscientizar os funcionários para que eles entendam os motivos sobre cada suas ações e práticas que devem ser seguidas dentro do âmbito organizacional, ter uma boa comunicação nas palestras para garantir o bom entendimento das práticas de cada um, palestras mensais antes do horário de trabalho, sempre reforçar o hábito de análise de possíveis riscos de cada área, conforme trecho da norma a seguir.

*Convém que todos os funcionários da organização e, onde pertinente, fornecedores e terceiros recebam treinamento apropriados em conscientização, e atualizações regulares nas políticas e procedimentos organizacionais, relevantes para as suas funções conforme a* ***ABNT NBR ISO/IEC 17799:2005.***

Ter um documento que contemple os treinamentos, compartilhar com os funcionários o ato da criação da PSI, ter este ciclo de treinamento documentado para a própria revisão dos funcionários. A parte pública desse documento com as rotinas devem ser entregues aos funcionários recém contratados pela empresa, para que eles se adequem as normas e práticas contidas no documento.

- Diga aos funcionários quais dados podem ser compartilhados com as pessoas de diferentes setores, ou externas à empresa.
- Sempre bloquear os computadores ao saírem de suas tarefas com relação à empresa
- Nunca passar as senhas para, mesmo que para colegas do trabalho
- Identificar possíveis situações de risco
- Sempre se atentar as atualizações de software
- Não entrar em redes sociais nos computadores corporativos, caso permitido, não divulgar nenhuma informação da empresa.
- Tomar extremo cuidado nos sites que entram com computadores corporativos, cuidado com downloads, bem como acessar e-mails duvidosos.
- Sempre reportar qualquer suspeita à equipe de T.I
- Instituir a política de criação de senhas fortes.
- Não permitir capturas de tela de documentos ou outro assunto relacionado à empresa
- Ter uma política para que apenas os gestores tenham acesso aos dados empresariais.

Após entender o que deve ser levado em consideração em um treinamento de usuários devemos adequá-lo na carga de trabalho inicial da equipe, reservar esse tempo para todos entender o que precisa ser seguido em uma rotina tradicional de trabalho, receber folhetos com as normas que devem ser seguidas. Ter exames após um período de testes para ter a garantia de que todos estão acompanhando e concordando com os métodos usados pela organização.

## 7.0 DIMINUIÇÃO DE RISCO

Com todo o treinamento realizado por nossa equipe, mudança para ambiente em nuvem, e ajustes de concessão de acessos dos usuários, foi possível mitigar a grande maioria das falhas de segurança da informação presente anteriormente nesta empresa.

### 7.1 AMBIENTE EM NUVEM AWS ESTAÇÕES E SERVIDORES

Com a migração das estações de trabalho e servidores para o ambiente AWS conseguimos reduzir os problemas com perdas de dados, e dados furtados, pois com o ambiente seguro da Amazon, se dá necessário para ter acesso aos dados um login e senha, assim construímos um ambiente altamente controlado.

O ambiente em nuvem teremos redundância de servidores e backup, com isso toda a informação está segura e tem disponibilidade total.

### 7.2 AJUSTE DE CONCESSÃO DE ACESSO

Com o ajuste de acesso, foi possível inibir problemas com licenciamento, e perigos a segurança da informação pois o ambiente está centralizado na nuvem AWS.

Foi feita toda a revisão de concessão para os usuários, hoje não é mais possível a instalação de qualquer software, pois as estações estão virtualizadas em nuvem, e para cada software que seja necessário para utilização, se dá a necessidade de ser passado pela aprovação do gestor do funcionário além da avaliação por parte da equipe de T.I.

Também foi realizada a instalação de um servidor proxy, com isso a navegação pode ser melhor controlada, com liberação de acesso *full* em determinados horários do dia, com isso facilitamos a administração por parte da equipe de segurança da informação.

### 7.3 TREINAMENTO E CONCIENTIZAÇÃO

Com o treinamento realizado pela nossa equipe boa tarde dos problemas com a segurança.

Foram realizados palestras e treinamentos para colaboradores a fim de conscientizar sobre os perigos de instalação de um software pirata, além de informarmos os perigos de navegação em sites não confiáveis.

Foi disponibilizado informações e artigos em uma Wiki interna para consulta por parte dos colaboradores caso haja dúvidas sobre os treinamentos aplicados.

## 8.0 CUSTO BENEFÍCIO

Investimos em um servidor em nuvem com valor mensal de R$2.000 para que a empresa tenha redução de custos com maquinário, atualmente as informações estão em um data center, assim não se fazendo a necessidade de custos com licenças de software, hardware e energia elétrica. Investimento em ThinClient no valor total de R$13.000 com objetivo de facilitar posteriores expansões na parte de máquinas, tem maior duração que um computador, capaz de se integrar com diferentes sistemas, e Controle de acesso ideal para empresas.

Investimento no software AmazonSpace no valor total de R$13.000 com foco em prover máquinas Windows ou Linux para vários funcionários que podem ser acessados de qualquer lugar e com qualquer dispositivo compatível, não oferece custos com gerenciamento de hardware.

Investimento no software SevenShop com valor mensal de R$1.000 visando maior administração e gerenciamento da empresa, tendo objetivos de melhorar as vendas, melhorar o gerenciamento do estoque, financeira e atendimento.

O sistema de vendas passa a ficar mais rápido através do código de barras permitindo várias formas de pagamento, manutenção do cadastro no mesmo lugar, contando com armazenamento em nuvem dos dados e controle de movimentação financeira, acesso com outras filiais através do SevenShop WEB, visão geral em tempo real de relatórios.

## 9.0 PUNIÇÕES

Todos os colaboradores, devem seguir as normas da segurança da informação, conforme treinamento realizado.

Serão aplicadas punições se as mesmas não forem seguidas corretamente, conforme as normas presente para implementação da PSI.

Para os colaboradores que não seguirem as normas estabelecidas, aonde é instruído o não compartilhamento de informações sigilosas, acessar sites proibidos, compartilhar senhas e prints de tela de informações corporativas, sejam elas senhas ou outros dados, conforme informado na ISO-27001 aonde solicita o sigilo será punido conforme as normas e leis a seguir.

Caso o funcionário infrinja as normas da empresa após advertência verbal e a advertência por escrito, o funcionário poderá receber uma suspensão de, no máximo, 30 dias (um mês). O prolongamento desse tempo é considerado punição excessiva nos termos do artigo 474 do Decreto-lei n° 5,452 de 01 de Maio de 1943 da CLT.

A dispensa por justa causa ocorre quando o empregado comete faltas graves, seguindo o artigo 482 do Decreto-lei n° 5,452 de 01 de Maio de 1943 da CLT, nesse caso o funcionário recebe o saldo do salário e os períodos de férias vencidas.

## 10.0 AVAL EQUIPE TECNICA

Para quais quer atividade na empresa quanto se condiz a área da informação é necessário o aval da área técnica com o objetivo de preservar a informação na empresa.

De acordo com a ISO/IEC 17799:2005, foi elaborado uma documentação com toda a fase da PSI que o projeto desencadeou.

Esse documento teve a aprovação de toda a diretoria e corpo técnico, para prosseguimento da implantação deste projeto para a Droga Rias LTDA.

## 11.0 PLANO DE CONTINUIDADE DO NEGÓCIO

Para o plano de continuação do negócios, temos o ambiente em Cloud Computer para os servidores que armazenam toda a informação da empresa.

Neste caso, os funcionários da área técnica foram instruídos a acompanharem em caso de desastre a troca de servidor que é automática devido ao mesmos estarem replicados em nuvem, assim não é necessário realizar a troca de contingência manualmente.

Em caso de perda de dados hoje o backup é realizado diariamente nos servidores, caso algum dado seja excluído indesejada mente, basta a área técnica seguir com as instrução passadas para restore de dados.

Para problemas de hardware nos Thincliente, em todas as unidades temos equipamentos de backup, desta forma caso tenhamos problemas, o equipamento pode ser substituído, e o envio do equipamento defeituoso deve ser realizado conforme instrução passada para área técnica.

# CONCLUSÃO

Com o projeto de implementação da PSI para o grupo Droga Rias LTD, concluímos que o ambiente está devidamente seguro e os funcionários devidamente qualificados para seguirem as normas da segurança da informação.

O projeto está cobrindo toda a parte de segurança lógica e física da segurança da informação.

Para a parte de segurança lógica, temos diversas camadas de segurança para a informação aonde existem controle de acessos dos usuários, controle de política de senha, controle de política de navegação.

Para a segurança física, os dados contidos nesta empresa, estão armazenados em servidores Cloud, aonde temos backups diários, replicação de servidores garantindo assim a total disponibilidade e segurança das informações.

Para a continuidade do negócio, aconselhamos sempre a empresa seguir a documentação disponibilizada para os mesmo, aonde contém todos os dados necessários para esta finalidade.

REFERÊNCIA BIBLIOGRÁFICA

WorkSpaces AWS

*https://aws.amazon.com/pt/workspaces/?nc2=type_a&workspaces-blogs.sort-by=item.additionalFields.createdDate&workspaces-blogs.sort-order=desc*

*Banco de dados AWS*

*https://aws.amazon.com/pt/free/database/*

*Software para gestão*

*http://www.sevenshop.com.br/index.php/sistema*

*Manual Amazon implantação de estações em nuvem*

*https://d1.awsstatic.com/Projects/provision-cloud-desktops/Provision%20Desktops%20in%20the%20Cloud%20-%20Implementation%20Guide.pdf*

PDF ISSO/IEC 17799

- *NORMA BRASILEIRA ABNT NBR ISO/IEC 17799 Segunda edição 31.08.2005 Válida a partir de 30.09.2005*