RELATÓRIO FINAL DE SEGURANÇA DA INFORMAÇÃO

Nome da instituição: Centro Universitário do Sul de Minas - UNIS MG

Nome do projeto: Projeto Extensionista de Segurança da Informação

Nome da empresa analisada: Jaguara Coffee

Nome dos autores (alunos): Ingryd De Lima, João Pedro Tavares Vicente, Lucas Silva Ciacci, Matheus Percker Donato Dos Santos, Victor Emanuel Souza Martins e Vinicius Henrique Andre Alves

Nome do(s) orientador(es): Ricardo Bernardes de Mello

1. Introdução

Este relatório integra as atividades desenvolvidas no Projeto Extensionista de Segurança da Informação do Centro Universitário do Sul de Minas – UNIS MG. O projeto tem como finalidade proporcionar aos alunos uma vivência prática aplicada, ao mesmo tempo em que contribui com a sociedade regional por meio de diagnósticos especializados em segurança da informação voltados para empresas locais.

A relevância social do projeto reside na crescente dependência das organizações em relação à tecnologia da informação e no consequente aumento dos riscos cibernéticos, que podem comprometer a continuidade dos negócios. Ao oferecer uma análise gratuita e técnica, o projeto promove maior conscientização sobre os riscos digitais, além de fomentar práticas de proteção mais eficazes, beneficiando tanto a empresa avaliada quanto a formação dos alunos envolvidos.

O objetivo deste relatório é apresentar os principais achados da análise realizada, incluindo a descrição da infraestrutura tecnológica da empresa, identificação de vulnerabilidades, mapeamento de riscos e sugestões de correções e melhorias. Além disso, será proposta uma política de segurança da informação compatível com a realidade observada.

A metodologia aplicada consistiu na elaboração e aplicação de dois formulários eletrônicos, desenvolvidos por meio do Google Forms. O primeiro formulário, com foco mais técnico, foi direcionado aos profissionais da área de Tecnologia da Informação da empresa. Já o segundo buscou capturar percepções e práticas relacionadas à segurança da informação por parte de colaboradores de diferentes setores. A combinação desses instrumentos possibilitou uma visão mais abrangente sobre o cenário de segurança da organização, com base tanto na estrutura tecnológica quanto no comportamento humano.

A análise foi realizada na empresa **Jaguara**, uma exportadora e fornecedora de cafés verdes especiais brasileiros, localizada na região do Campo das Vertentes. A

empresa se destaca por práticas sustentáveis, inovações no cultivo e comercialização de cafés, e vem ganhando reconhecimento internacional por sua qualidade e compromisso com o meio ambiente. A atuação da área de TI, embora enxuta, é estratégica para sustentar a inovação e a eficiência dos processos.

2. Infraestrutura Tecnológica

2.1 Hardware

A empresa possui atualmente:

- **8 notebooks com sistema operacional Windows 11 licenciado**, utilizados pelos colaboradores em suas atividades rotineiras;
- **1 modem da operadora Vivo** para acesso à internet;
- **1 roteador Multilaser**, responsável pela distribuição de rede interna;
- **8 celulares pessoais**, utilizados também para atividades de trabalho, uma vez que a empresa não fornece aparelhos corporativos.

Toda a infraestrutura de hardware está sob responsabilidade da área de TI, que realiza a manutenção, suporte técnico e aquisição de equipamentos conforme necessidade.

2.2 Software

Os softwares utilizados na empresa são:

- **Sistema operacional:** Windows 11 (licenciado);
- **Navegador padrão:** Google Chrome;
- **Softwares empresariais:** Sistemas terceirizados voltados ao controle de armazéns e gerenciamento da qualidade do café;
- **Antivírus:** A empresa **não utiliza nenhum sistema de antivírus atualmente**;
- **Armazenamento e colaboração:** Para documentos pessoais, os colaboradores utilizam o **OneDrive**. Já para arquivos compartilhados, utiliza-se o **Google Drive**;
- **Outros serviços SaaS:** A empresa também utiliza o **Google One** e o **Office 360**, principalmente para produtividade e gestão documental.

2.3 Telecomunicações

- A conexão com a internet é fornecida exclusivamente pela operadora **Vivo**.
- **Não há redundância de operadoras** ou links de internet, o que representa um ponto crítico em caso de falhas na conectividade.
- A banda de internet contratada e a estabilidade da conexão não foram especificadas diretamente, mas foram apontadas como fatores relevantes para futuras análises de desempenho.

2.4 Recursos Humanos de TI
A equipe de TI é composta por 1 profissional que responde por toda a estrutura tecnológica da empresa. Suas principais responsabilidades incluem:

- Desenvolvimento e manutenção do site da empresa;
- Suporte técnico aos equipamentos dos colaboradores (manutenção, formatação, substituição);
- Gestão e manutenção da infraestrutura de rede;
- Pesquisa e aplicação de **inovações tecnológicas voltadas à produção e comercialização de cafés especiais**.

3. Vulnerabilidades Identificadas

Durante a análise da empresa Jaguara, foram identificadas diversas fragilidades nos processos e recursos tecnológicos, com base nas respostas obtidas via formulários e planilha técnica de levantamento. As vulnerabilidades estão relacionadas a aspectos técnicos, operacionais e humanos, e podem ser agrupadas da seguinte forma:

3.1 Controle de Acesso e Autenticação

- **Compartilhamento de senhas entre usuários**, prática comum no ambiente interno.
- **Senhas fracas e reutilizadas**, sem exigência de critérios mínimos de complexidade.
- **Falta de alinhamento entre RH e TI para desativação de contas de ex-funcionários**, o que permite acessos indevidos após o desligamento.

3.2 Infraestrutura Física e Estações de Trabalho

- **Cabeamento e equipamentos expostos**, sem organização ou proteção adequada.
- **Racks de rede abertos**, vulneráveis a acesso físico não autorizado.
- **Estações de trabalho deixadas desbloqueadas durante ausências**, aumentando risco de manipulação indevida.

3.3 Permissões e Privacidade

- **Permissões excessivas** em determinadas áreas (ex: Departamento de Pessoal), contrariando o princípio do menor privilégio.

3.4 Backup e Restauração de Dados

- **Ausência de política centralizada de backup**; a responsabilidade recai sobre o próprio colaborador.

- **Backups não automatizados e sem testes regulares**, o que coloca em risco a recuperação de dados em caso de falhas ou ataques.

3.5 Monitoramento e Logs

- **Falta de logs detalhados** de ações dos usuários e de acesso a sistemas, o que dificulta auditorias e investigações.

3.6 Conscientização e Cultura de Segurança

- **Ausência de treinamentos formais** sobre segurança da informação.
- **Desconhecimento sobre golpes digitais (ex: phishing)** por parte dos funcionários.
- **Falta de simulações e reforço contínuo** para desenvolvimento de boas práticas no dia a dia.

Essas vulnerabilidades foram classificadas posteriormente com base em sua gravidade, impacto e probabilidade de ocorrência, sendo detalhadas nos próximos tópicos com mapeamento de riscos, sugestões de correção e melhorias estruturais.

4. Mapeamento de Riscos

Descrição do Risco	Causa	Impacto	Probabilidade	Nível do Risco	Área Afetada	Observações
Compartilhamento de senhas	Prática informal entre supervisores e funcionários	Acesso indevido a dados confidenciais	Alta	Alto	Controle de Acesso	Relato de fornecimento de senhas a novos colaboradores
Senhas fracas e reutilizadas	Ausência de política de senhas robusta	Comprometimento de contas por força bruta ou vazamento	Alta	Alto	Segurança da Informação	Não há exigência de senhas fortes ou políticas de troca
Contas de ex-funcionários ativas	Falta de comunicação entre RH e TI	Acesso indevido após desligamento	Média	Alto	Recursos Humanos / TI	Risco de manipulação de dados sensíveis
Equipamentos de rede expostos	Falta de organização e proteção física	Danos acidentais ou acesso físico não autorizado	Média	Médio	Infraestrutura Física	Cabeamentos e rack de rede desprotegidos
Estações desbloqueadas em ausências	Falta de bloqueio automático	Acesso indevido a sistemas e documentos	Alta	Alto	Usuário final	Observado que usuários deixam PCs abertos durante pausas
Permissões excessivas em sistemas	Ausência de revisão de permissões	Alterações indevidas em configurações e dados	Média	Alto	Setores administrativos	Departamento de Pessoal com acesso irrestrito
Falta de política de backup centralizada	Backup feito de forma individual e não sistemática	Perda de dados críticos	Alta	Alto	TI / Toda empresa	Backups não são automatizados e não há testes
Ausência de logs de ações	Sistema não registra ações detalhadas dos usuários	Dificuldade em auditorias e investigações	Média	Médio	Sistemas / Segurança	Apenas registros básicos de entrada e saída
Falta de treinamento em segurança	Inexistência de ações de conscientização	Vulnerabilidade a ataques sociais (phishing, engenharia social)	Alta	Alto	Todos os colaboradores	Não há treinamentos ou simulações
Sistemas aceitam dados inválidos	Falta de validação nas entradas	Relatórios incorretos e falhas operacionais	Média	Médio	Sistemas internos	Campos de data e informação sem verificação

5. Sugestões de Correções

Vulnerabilidade	Solução Recomendada
Compartilhamento de senhas entre colaboradores	Implementar autenticação individual obrigatória com senhas únicas e treinamento sobre a importância da confidencialidade das credenciais
Utilização de senhas fracas e repetidas	Criar e aplicar uma política de senhas fortes com exigência de letras maiúsculas/minúsculas, números e símbolos; definir prazo de validade para troca periódica
Contas de ex-funcionários não desativadas	Estabelecer processo formal de comunicação entre RH e TI para desativação imediata de acessos após desligamento
Equipamentos de rede expostos (modem, roteador, cabos)	Reorganizar e proteger fisicamente os equipamentos de rede com racks fechados e sinalização adequada
Computadores desbloqueados durante ausência do usuário	Configurar bloqueio automático de tela após inatividade e orientar usuários sobre a responsabilidade no uso dos equipamentos
Permissões excessivas em sistemas internos	Aplicar o princípio do menor privilégio, revisando as permissões de acesso periodicamente com base na função de cada colaborador
Ausência de política centralizada de backup	Implantar política de backup automatizado com armazenamentos em nuvem e testes periódicos de recuperação
Falta de logs detalhados de ações em sistemas	Adotar sistemas que ofereçam rastreamento completo de ações dos usuários (logs de atividade, acessos, alterações)
Ausência de treinamentos sobre segurança da informação	Realizar treinamentos periódicos e ações de conscientização para toda a equipe sobre riscos digitais e boas práticas
Sistemas aceitando entradas inválidas (ex: datas incorretas)	Implementar mecanismos de validação de dados nos sistemas utilizados para evitar erros operacionais

6. Oportunidades de Melhoria da Infraestrutura Tecnológica

1. Implantação de ferramentas de monitoramento e gerenciamento de rede

- Adotar soluções que permitam o acompanhamento em tempo real do tráfego de rede, acessos e status dos equipamentos.

- Benefício: maior visibilidade e agilidade para identificar falhas, intrusões ou uso indevido de recursos.

2. Adoção de antivírus corporativo com painel de gerenciamento centralizado

- Substituir o cenário atual de ausência de antivírus por uma solução robusta com controle central.
- Benefício: proteção contra malware, ransomware e vulnerabilidades exploráveis por dispositivos externos.

3. Expansão e capacitação da equipe de TI

- Avaliar a necessidade de apoio técnico ao profissional responsável pela TI, especialmente em momentos críticos.
- Benefício: melhora na resposta a incidentes, execução de projetos de melhoria e inovação.

4. Criação de um plano de continuidade de negócios e recuperação de desastres

- Desenvolver um plano formal, com procedimentos de resposta a falhas graves, ataques cibernéticos ou indisponibilidade de sistemas.
- Benefício: maior preparo para situações de crise e menor tempo de recuperação.

5. Revisão e padronização da arquitetura de rede

- Organizar os equipamentos de rede (modem, roteador, cabos) em um ambiente estruturado, com cabeamento adequado e segmentação lógica da rede.
- Benefício: melhora de desempenho, estabilidade e segurança da rede.

6. Investimento gradual em serviços de nuvem mais seguros e escaláveis

- Avaliar a migração de serviços internos para soluções cloud mais estruturadas, como Google Workspace ou Microsoft 365 Business.
- Benefício: confiabilidade, disponibilidade, backup integrado e recursos colaborativos avançados.

7. Implementação de um sistema de gestão de TI ou controle de ativos

- Adotar uma ferramenta simples para registrar, acompanhar e auditar os equipamentos e softwares utilizados pela empresa.
- Benefício: organização, histórico de manutenções e planejamento de reposições.

8. Criação de um cronograma fixo de treinamentos em segurança da informação

- Estabelecer uma rotina de capacitação para novos e antigos colaboradores, com conteúdos adaptados à realidade da empresa.
- Benefício: formação de uma cultura de segurança contínua e colaborativa.

7. Política de Segurança da Informação (Sugestão)

7.1 Objetivo

Esta política tem como objetivo estabelecer diretrizes e normas para assegurar a proteção das informações da empresa Jaguara, preservando sua **confidencialidade, integridade e disponibilidade**, além de reduzir os riscos associados ao uso inadequado de recursos tecnológicos.

7.2 Escopo

Esta política se aplica a todos os colaboradores da empresa, independentemente do cargo ou área de atuação, bem como a terceiros, parceiros e prestadores de serviço que tenham acesso aos sistemas, informações ou equipamentos da organização.

7.3 Diretrizes Gerais

- Todos os colaboradores são responsáveis por zelar pelas informações e recursos tecnológicos da empresa.
- O acesso às informações deve ser restrito conforme a função e necessidade de cada colaborador.
- É proibida a instalação de softwares não autorizados ou de procedência duvidosa.
- Toda atividade que envolva dados sensíveis deve ser realizada com critérios de segurança definidos por esta política.

7.4 Controle de Acesso

- Cada colaborador deve possuir credenciais individuais de acesso aos sistemas.
- É **terminantemente proibido** o compartilhamento de senhas ou contas de usuário.
- Os acessos devem ser concedidos com base no princípio do menor privilégio.
- Contas de usuários devem ser desativadas imediatamente após o desligamento do colaborador.

7.5 Política de Senhas

- As senhas devem conter **no mínimo 12 caracteres**, com letras maiúsculas, minúsculas, números e símbolos.
- Recomenda-se a troca periódica de senhas a cada **90 dias**.
- Senhas não devem ser anotadas em papel ou salvas em arquivos não protegidos.
- É vedado o uso de senhas já utilizadas anteriormente.

7.6 Backup e Recuperação de Dados

- Os dados corporativos devem ser salvos em ambientes de armazenamento seguros, preferencialmente em nuvem (OneDrive, Google Drive, Google One).
- O processo de backup deve ser automatizado e executado **diariamente**.
- Testes periódicos de recuperação devem ser realizados para garantir a integridade dos backups.
- O responsável técnico da TI deve monitorar e manter os registros de backup.

7.7 Uso de Equipamentos e Recursos

- Equipamentos fornecidos pela empresa são de uso exclusivo para fins profissionais.

- O uso de dispositivos pessoais (BYOD) para atividades da empresa deve ser autorizado e acompanhado pelo setor de TI.

- Os dispositivos devem permanecer bloqueados sempre que o usuário se ausentar.

- É vedada a conexão de pen drives ou dispositivos não verificados sem autorização.

7.8 Conscientização e Treinamento

- Todos os colaboradores devem participar de **treinamentos periódicos** sobre segurança da informação.

- Devem ser promovidas campanhas internas de conscientização sobre ameaças como **phishing, engenharia social, malwares** e boas práticas de segurança digital.

- Novos colaboradores devem receber orientações iniciais sobre esta política no processo de integração.

7.9 Registro e Monitoramento

- Todos os sistemas devem manter **logs de acesso e atividades críticas** de forma segura e organizada.

- Os registros devem permitir a rastreabilidade de ações realizadas por usuários.

- A retenção mínima dos logs deve ser de 6 meses.

7.10 Resposta a Incidentes

- Qualquer colaborador que identifique uma falha ou incidente de segurança deve comunicar imediatamente o responsável pela TI.

- A equipe técnica será responsável por analisar, conter e documentar o incidente.

- Casos graves devem ser avaliados com medidas corretivas, preventivas e, quando necessário, comunicação à direção.

7.11 Penalidades

O descumprimento das diretrizes estabelecidas nesta política poderá acarretar:

- Advertência verbal ou escrita;
- Restrição de acessos;
- Medidas disciplinares conforme previsto no regulamento interno da empresa;
- Em casos extremos, rescisão contratual ou ação judicial.

7.12 Atualização da Política

Esta política deve ser revisada **anualmente** ou sempre que houver mudanças significativas na estrutura tecnológica da empresa. A responsabilidade pela atualização é do responsável pela área de Tecnologia da Informação, em conjunto com a gestão administrativa.

8. Considerações Finais

A análise realizada na empresa Jaguara permitiu identificar uma série de vulnerabilidades e oportunidades de melhoria em sua infraestrutura tecnológica e nas práticas relacionadas à segurança da informação. Por meio da aplicação de formulários direcionados e da análise técnica das respostas, foi possível traçar um diagnóstico realista, abrangente e construtivo, respeitando a dinâmica e o porte da organização.

A adoção das recomendações propostas neste relatório tende a trazer benefícios significativos para a empresa, como a **redução de riscos operacionais**, a **proteção contra vazamento de informações sensíveis**, **maior controle sobre acessos e dados** e a formação de uma **cultura de segurança sólida e contínua**. Além disso, investimentos em melhorias estratégicas podem elevar o nível de maturidade tecnológica da empresa, tornando-a mais preparada para os desafios do ambiente digital atual.

Para os alunos envolvidos no projeto, a experiência proporcionou uma vivência concreta da aplicação dos conhecimentos adquiridos em sala de aula. A interação com uma realidade empresarial, a análise de um ambiente real e a elaboração de soluções

práticas fortaleceram o desenvolvimento técnico, crítico e profissional dos participantes, ampliando sua visão sobre os desafios da cibersegurança e da gestão de tecnologia da informação.

Por fim, ressalta-se a importância do envolvimento da empresa nesse processo. A abertura para colaborar com o projeto, fornecer informações e refletir sobre sua própria estrutura tecnológica demonstra um compromisso genuíno com a melhoria contínua e com a proteção dos dados e ativos que sustentam seu negócio. Essa parceria entre instituição de ensino e empresa reforça o papel social da extensão universitária e gera resultados positivos para todos os envolvidos.