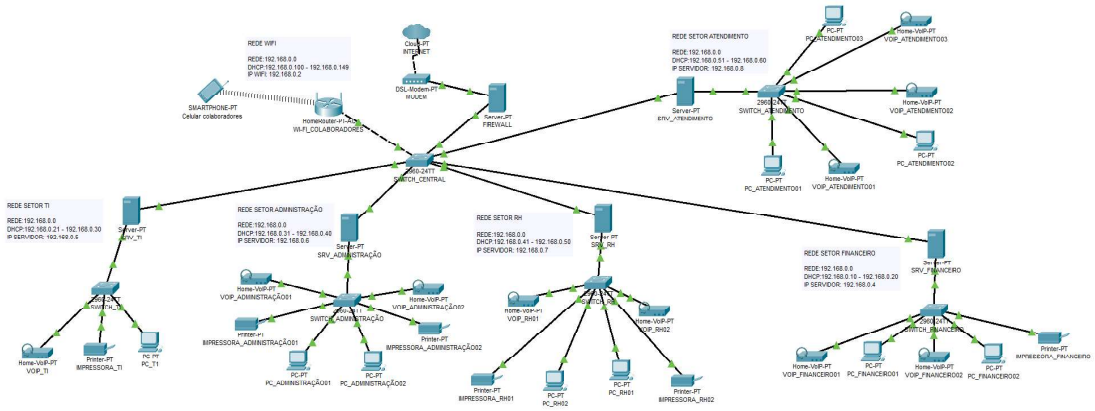
Na imagem abaixo, podemos observar como foi feita a distribuição dos IPs de cada equipamento:



Para melhor vizualização da imagem, disponibilizamos um arquivo em nuvem: https://drive.google.com/drive/folders/1b9Xx8Xr_JwIzmganHxUymkR83fe9V6nK?usp=drive_link

3.5. Segurança da Informação

3.5.1. Análise de Riscos

3.5.1.1. Identificação e Avaliação dos Riscos de Segurança para a Empresa

Inventário → Ativos de informação da organização, incluindo hardware, software, dados e pessoas.

Valor → Valor de cada ativo, considerando o impacto potencial da sua perda ou comprometimento.

Riscos → Priorizar os riscos com base em sua gravidade. Avaliando a probabilidade de ocorrência de cada ameaça, (alta, média, baixa).

3.5.1.2. Análise de Vulnerabilidades e Ameaças Potenciais

- Ameaças → Erros humanos, falhas de sistema.
- Tipos de Ameaças → Hackers, concorrentes, Malware
- Fraquezas → Identificar fraquezas nos sistemas e processos que podem ser exploradas por ameaças.
- Efetuar simulações de ataques para identificar vulnerabilidades não descobertas.

3.5.2. Implementação de Medidas de Segurança

3.5.2.1. Implementação de Políticas de Controle de Acesso aos Sistemas e Dados

Permissões→ Administrador, gerente, usuário, diretoria.

Controle de Acesso → Utilizar sistemas de Gestão de Identidade e Acesso (I. A)

Identificar → classificar os sistemas com, aplicativos e dados.

Plano de Emergência → Definir procedimentos para responder a acessos não autorizados e estabelecer equipes de resposta.

Configuração de sistemas de detecção de intrusão e prevenção de ataques:

Instalação de Sistemas → **Configuração do sistema, incluindo definição de parâmetros básicos e integração com a infraestrutura existente.**

IDS/IPS → **Decida entre um IDS/IPS baseado em rede (NIDS/NIPS) e um baseado em host (HIDS/HIPS)**

Infraestrutura → Infraestrutura de rede para determinar onde colocar os sensores

Segurança → Políticas claras sobre o que constitui atividade suspeita e quais ações devem ser tomadas em resposta

Logs → logs para identificar padrões e investigar incidentes.

Manutenção e Atualizações → Mantenha as assinaturas e regras do IDS/IPS atualizadas para se proteger contra novas ameaças, configurações do sistema para adaptá-lo a mudanças na infraestrutura e nas ameaças

Revisões Semanal → Realize revisões do sistema e das políticas para garantir que continuam eficazes e atualizadas.

Riscos Identificados:

- Ameaça: Vulnerabilidade de Softwares
  - Impacto: Alto
  - Probablilidade: Alto

- Ameaça: Malware
  - Impacto: Alto
  - Probablilidade: Médio

- Ameaça: Ataque DDOS
  - Impacto: Médio
  - Probablilidade: Alto

- Ameaça: Ameaças Internas
  - Impacto: Médop
  - Probablilidade: Baixo

- Ameaça: Senhas
  - Impacto: Alto
  - Probablilidade: Alto

- Ameaça: Dados Vasados
  - Impacto: Alto
  - Probablilidade: Alto

- Ameaça: SQL
  - Impacto: Alto
  - Probablilidade: Médio

- Ameaça: Ataques
  - Impacto: Médio
  - Probablilidade: Médio

- Ameaça: Infiltração de Dados
  - Impacto: Alto
  - Probablilidade: Alto

- Ameaça: Cavalo de Troia
  - Impacto: Médio
  - Probablilidade: Médio

- Ameaça: Ataques via Bluetooth
  - Impacto: Baixo
  - Probablilidade: Baixo

- Ameaça: Ataques via Wi-fi
  - Impacto: Baixo
  - Probablilidade: Médio

- Ameaça: Serviços Nuvem
  - Impacto: Alto
  - Probablilidade: Alto

- Ameaça: Patches Incompletos
  - Impacto: Baixo
  - Probablilidade: Baixo

- Ameaça: Segurança Fraca
  - Impacto: Alto
  - Probablilidade: Alto

- Ameaça: Protocolos de Rede
  - Impacto: Baixo
  - Probablilidade: Baixo

- Ameaça: Scrip
  - Impacto: Baixo
  - Probablilidade: Baixo

- Ameaça: Ataques de Redirecionamento
  - Impacto: Médio
  - Probablilidade: Médio

- Ameaça: Configurações de Seguranças incompletas e incorretas
  - Impacto: Alto
  - Probablilidade: Alto

- Ameaça: Falsificação de Identidade
  - Impacto: Alto
  - Probablilidade: Alto

Politicas de Acesso

- **Controle de acesso a sistemas**:
  - O acesso a sistemas de controle como sistemas de automação, para proteger infraestruturas críticas contra ameaças cibernéticas.

- **Revisão de acesso regular**:
  - Revisar e atualizar regularmente as permissões de acesso dos usuários

- **Dispositivos Móveis**:
  - Acesso seguro a recursos da organização por meio de dispositivos móveis, como Celulares e tablets.

- **Rede sem Fio**:
  - Seguranças específicas para redes sem fio, como autenticação WPA2/WPA3, controle de acesso e de rede

- **Privilégios**:
  - Conceder acesso mínimo para que os usuários realizem suas funções

- **Senhas**:
  - Estabelecer caracteres para senhas, incluindo comprimento mínimo, alteração regular de senhas

- **Tentativas de Acessos**:
  - Bloquear temporariamente após um número específico de tentativas de login.

- **Acesso somente horário de trabalho ou autorizado fora do expediente**:
  - Limitar o acesso a determinados recursos ou sistemas com base no horário do dia ou na carga horaria de trabalho dos usuários.

- **Terceiros tentando acessar login e senha de outro funcionário**:
  - Estabelecer protocolos para conceder e revogar o acesso de fornecedores, parceiros e outras externas.

- **Documentos e Arquivos**:
  - Permitir acessos específicos sobre documentos e arquivos, incluindo compartilhamento seguro e edição.

3.5.2.2. Configuração de Sistemas de Detecção de Intrusão e Prevenção de Ataques

Instale e Configure sistemas para detectar e prevenir intrusões

- Ajustes e aprimoramento
- Manutenção e Supervisão
- Treinamento.
- Testes e validações
- Configuração do sistema.
- Instalação do sistema.
- Escolha o sistema.

Medidas de detecção e prevenção de ataques na empresa

- **Análise de comportamento do usuário**:
  - Análise comportamental de usuários para identificar desvios de padrões normais de comportamento que possam indicar atividade irregular

- **Atualizações de segurança**:
  - Sistemas e softwares atualizados com os patches de segurança mais recentes para corrigir novos e velhos erros

- **Treinamento de segurança**:
  - Treinamento regular em segurança para funcionários, sobre práticas seguras de computação e como identificar possíveis ameaças.

- **Acesso a páginas Web**:
  - Filtros de conteúdo da web para bloquear o acesso a sites maliciosos conhecidos e downloads de arquivos perigosos.

- **Antivirus**:
  - Antivírus atualizados em todos os dispositivos da empresa para detectar e remover software

- **Rede**:
  - Divida a rede em segmentos menores e restrinja o tráfego entre eles, limitando assim o alcance de ataques indevidos

- **Acesso de usuarios**:
  - Monitorando as atividades dos usuários com acessos elevados para detectar qualquer comportamento diferente da politica da empresa.

- **Dados**:
  - Utilizando o sistema de criptografia para proteger dados confidenciais armazenados e transmitidos.

- **Trafego de dados**:
  - Criptografia para proteger a integridade das comunicações, especificamente em redes Wi-Fi, redes públicas ou não confiáveis.

- **Backup**:
  - Realizar diariamente backups de dados e testes, testando a capacidade de restauração para garantir contra-ataques de hackers e perda de dados.

- **Email**:
  - Criar filtro para os e-mails da empresa, assim podendo identificar e bloquear e-mails de malware e spam, gerando alerta para o T.I antes que alcancem as caixas de entrada dos usuários.

4. CONCLUSÃO

Com base nas nossas pesquisas, podemos afirmar que a nossa empresa possui uma grande variedades de se consolidar com as técnicas atribuídas durante a criação do projeto. Todas as matérias foram interligadas para a construção da Loccar.

O que podemos afirmar é que, extraimos o máximo de informações possíveis para o escopo e conclusão do que foi proposto a todos. Podemos afirmar que a Loccar possui tudo o que uma empresa deve ter para se firmar no grande mercado de locadoras de carros, batendo de frente com a concorrência.

O projeto em si nos deixou um grande aprendizado, pois ele nos ensinou a como integrar novas linguagens, novos temas dentro da área de T.I, e também a como extrair diversas informações com a mais grande quantidade de códigos váriados. Agradecemos todos os professores pelos ensinamentos a qual nos foi passado.

Esperamos que com a finalização do trabalho, possamos amadurecer como profissionais dentro da área, e claro, como pessoas também. Agradecemos a Uninove pela oportunidade.

5. REFERÊNCIAS

COELHO, Beatriz. **Entenda como fazer a conclusão do TCC corretamente.** 2017 Disponível em:
< https://rockcontent.com/br/blog/referencia-de-site-abnt/> acesso em: 13 de Mai.2024.

COELHO, Taysa. **7 sites para fazer planta baixa online grátis e fáceis de usar.** Disponível em:
< https://www.appgeek.com.br/planta-baixa-online/> acesso em: 09 de Abril.2024.

PASSARIN, Leonardo**. Resumo da ISO 27001 – Sistema de Gestão de Segurança da Informação**. 2021**.**
Disponível em:
< https://www.estrategiaconcursos.com.br/blog/resumo-da-iso-27001/> acesso em: 29 de Mar. 2024.

GuiaViajarMelhor. **Como funciona o aluguel de carros: 15 dúvidas comuns na hora de locar um veículo.** 2020.
Disponível em:
< https://guiaviajarmelhor.com.br/como-funciona-o-aluguel-de-carros-15-duvidas-comuns-na-hora-de-locar-um-veiculo/> acesso em: 27 de Fev. 2024.