PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
PUC Minas Virtual

Danilo Costa da Silva Figueredo – 855798
Guilherme Ferrari de Camillo – 844747
Heberson de Oliveira – 845399
José André Silva de Goes – 852104
Lucas Fernandes – 850985
Sérgio Rosa – 857111
Yasmin Fernandes – 792720

REAL MOTO PEÇAS:

subtítulo (em minúsculo, centralizado)

Belo Horizonte

2024

Nome completo dos autores

TÍTULO (EM MAIÚSCULO, CENTRALIZADO):
subtítulo (em minúsculo, centralizado)

Natureza do trabalho: recuado a 7cm. Fonte: tamanho 12. Espaço entre linhas simples.

Orientador: Nome completo

Belo Horizonte
2024

SUMÁRIO

1. INTRODUÇÃO (Etapa 4)

- Contextualize com informações sobre a organização e justifique sobre o processo de segurança a informação (apresente a demanda em no máximo três parágrafos).
- Faça uma síntese dos principais pontos do diagnóstico.

2. OBJETIVOS

2.1 Objetivo Geral

- Apresentar a visão dos processos de negócios organizacionais que envolvem a segurança das informações organizacionais.

2.2 Objetivos Específicos

- Identificar e analisar o contexto do negócio
- Classificar os itens das principais normas de segurança da informação.
- Mapear e modelar os processos de negócios da empresa.
- Modelar um sistema de informação baseado nos processos da empresa.
- Construir uma topologia de rede para a empresa.
- Avaliar o impacto cultural, religião na empresa em questão.
- Desenvolver um projeto de intervenção da estrutura organizacional utilizando métodos ágeis de gerência de projetos.
- Propor melhorias no processo de segurança da informação

Observação: a fim de desenvolver um planejamento eficiente sobre a definição do problema e objetivos do trabalho, fique atento às informações que serão levantadas. Pois um levantamento de informações ruins, levarão a análises ruins. Então, busque variáveis confiáveis para o desenvolvimento do projeto.

3. DIAGNÓSTICO ORGANIZACIONAL (Etapa 1)

3.1 Histórico da Organização

A Real Moto Peças é uma empresa de grande porte que atua na distribuição de autopeças, acessórios e moto peças em todo o território nacional. Fundada em 1962 na cidade de Uberlândia, Minas Gerais, pelos irmãos João e Otahyde Gomides.

Atualmente a Real Moto Peças integra o Grupo Real junto de outras duas empresas, a Disape, que também atua na distribuição de autopeças e acessórios, e a Mide Parts, marca própria de auto e acessórios.

Hoje, o Grupo Real conta com mais de 24 filiais localizadas em todo o país e com uma equipe multidisciplinar composta por cerca de 1.800 colaboradores, com operações divididas em diversas áreas do segmento de reposição, se destacando pela excelência em logística e entrega, atendimento personalizado de vendas, engajamento com a comunidade e visão transformadora de negócios com consultores externos personalizados que visitam e auxiliar no desenvolvimento de negócios dos parceiros.

A missão da empresa é prover as melhores soluções e inovações para a mobilidade das pessoas e produtos, através da distribuição de serviços. A Real tem como visão ser referência mundial na transformação do mercado de reposição e tem como valores fundamentais a ética, pessoas, excelência, colaboração e simplicidade.

Características básicas da segurança da informação:

O departamento de TI da Real Moto Peças é composto por 16 profissionais, sendo 12 da área de TI e 4 da área de Segurança da Informação. A equipe realiza de forma rotineira avaliação do status de segurança da rede e dos dispositivos tecnológicos da empresa.

Anualmente, o departamento de TI realiza treinamentos voltados para a área de segurança da informação. Ainda atua na Real Moto Peças, de forma terceirizada, uma empresa para a realização de testes de segurança como, por exemplo, phishing.

A Real Moto Peças possui uma Política de Segurança da Informação no qual são listadas as diretrizes para mitigação de riscos e incidentes. O documento abrange todos os colaboradores, fornecedores e parceiros que, de alguma forma, lidam com os dados e sistemas da empresa

Problemas de segurança da informação relatados pelo gestor:

- Shadow IT
- Baixa adesão de cultura de “segurança da informação” na empresa
- Mitigação de riscos de acesso à rede via VPN (colaboradores e terceiros)
- Melhorias na segurança de rede com a utilização do clearpass
- Educação dos usuários sobres cibersegurança através de gamificação

Mecanismos e tecnologias utilizados no processo de segurança:

Tecnologias

- Fortinet FortiGate 30E Network - Security/ Firewall Appliance
- CrowdStrike
- Antivirus Rapid7
- LanSweeper

Processos

- Zero Trust
- Treinamento de equipes

Processos que envolvem a organização:

Compras

O sistema monitora regularmente o estoque do produto e dispara para o setor responsável a informação sobre o pedido de unidades necessárias.

Vendas

São feitas por telefone e whatsapp e apenas para CNPJ. O sistema de estoque identifica a disponibilidade dos produtos e, caso positivo, confirma a reserva do produto, aguardando a confirmação de compra/pagamento. Em caso de indisponibilidade, de acordo com a quantidade de itens solicitados, o sistema de estoque gera um pedido de aquisição para o setor de compras. Os acessos são restritos conforme o setor que o funcionário está alocado, para fazer uma mudança no cadastro do cliente, apenas quem tem trabalha no setor de cadastro consegue fazer essas mudanças, para os vendedores, é liberado o acesso apenas a telas de venda e cotação.

Representante

O pedido é enviado pelo representante

Marketing

Alinhado com o setor financeiro da Real Moto Peças, o setor de Marketing define prioridades de investimento em publicidade semestralmente. O gerente do setor monitora por meio do sistema de registro de vendas e estoque, as principais forças e fraquezas do desempenho de comercialização de peças.

Financeiro

Após o pedido de compras ser feito e a nota ser emitida, o financeiro realiza o pagamento através do sistema ERP.

Entregas

Algemas empresas de logística fazem as entregas, existe a opção de retirada no local e algumas filiais possuem serviço de moto entrega.

Clientes

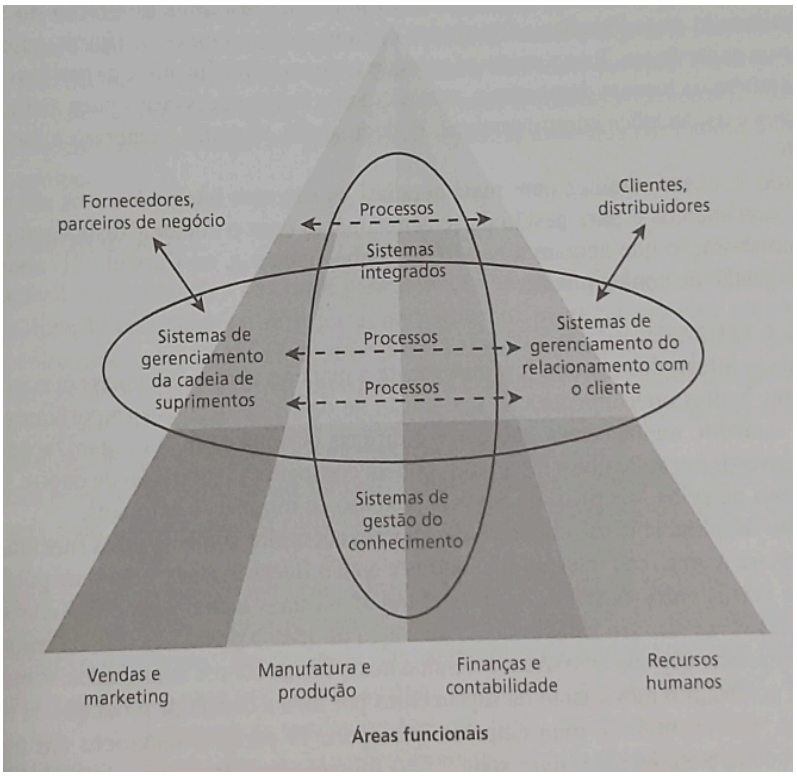
Os dados dos clientes registrados são mantidos sob registro, seguindo as indicações legais da LGPD. Apenas os usuários do respectivo setor de Vendas têm acesso ao tratamento desses dados com objetivos específicos de verificarem status relacionados à comercialização dos

produtos. Também seguindo a LGPD, tais dados são removidos do sistema de acordo com a solicitação do usuário.

Fornecedores

O sistema de ERP é fechado dentro da rede, quando o vendedor fecha o pedido um boleto é emitido e enviado diretamente para o email do cliente, com todas as informações necessárias.

3.2 Sistemas de Informação identificados na empresa



Fonte: LAUDON (2014, p.51)

Exemplo:

Software	Setor	Descrição
Sistema Sênior	RH	Registro de dados relativos aos colaboradores da empresa.
CrowdStrike	TI	Monitoramento de ameaças internas e externas
AntiVirus Rapid7	TI	Monitoramento de ameaças internas e externas
LanSweeper	TI	Inventário de usuários, dispositivos e software

MODELAGEM DO PROCESSO DE NEGÓCIO

Mapeamento dos processos atuais/existentes da empresa

A Real Moto Peças, como descrito anteriormente, é uma empresa de grande porte com diversas áreas funcionais. O foco deste mapeamento é nos processos relacionados à segurança da informação, identificando as entradas, saídas, recursos e a sequência de atividades.

Processos de Segurança Identificados:

1. **Gestão de Acesso à Rede**:

- **Entrada**: Credenciais de acesso dos funcionários e terceiros.
- **Saída**: Controle de acesso à rede e sistemas críticos da empresa.
- **Recursos**: VPN, sistemas de autenticação e Firewalls
- **Sequência de Atividades**:
  - Solicitação de acesso pela equipe ou terceiros.
  - Validação das credenciais.
  - Concessão de acesso monitorado.

2. **Treinamentos em Segurança da Informação**:
   - **Entrada**: Funcionários e colaboradores que acessam a rede e manipulam dados.
   - **Saída**: Colaboradores treinados para identificar riscos como phishing e proteger dados.
   - **Recursos**: Treinamentos anuais, sistemas de gamificação.
   - **Sequência de Atividades**:
     - Convocação de funcionários para treinamentos.
     - **Realização de testes de segurança, como phishing.**
     - Feedback e avaliação dos resultados dos testes.
3. **Monitoramento de Ameaças Internas e Externas**:
   - **Entrada**: Atividades de rede e tráfego de dados.
   - **Saída**: Relatórios de ameaças detectadas e ações corretivas.
   - **Recursos**: CrowdStrike, Rapid7, LanSweeper.
   - **Sequência de Atividades**:
     - Monitoramento contínuo da rede.
     - Identificação de atividades suspeitas.
     - Adoção de medidas corretivas quando ameaças são detectadas.
4. **Gerenciamento de Shadow IT**:
   - **Entrada**: Softwares não autorizados utilizados por funcionários.
   - **Saída**: Riscos identificados e mitigados.
   - **Recursos**: CrowdStrike, Firewalls.
   - **Sequência de Atividades**:
     - Detecção de softwares e aplicativos não autorizados.
     - **Avaliação do risco e impacto na segurança da rede.**
     - Implementação de bloqueios e medidas corretivas.

4.2. Proposta de melhorias nos processos de segurança da informação

Após o mapeamento dos processos atuais, algumas etapas redundantes e gargalos foram identificados, permitindo a formulação de sugestões para otimizar esses processos:

1. **Melhoria na Gestão de Acesso**:
    - **Problema**: A gestão de credenciais é suscetível a riscos, especialmente para colaboradores remotos e terceiros.
    - **Solução Proposta**: Implementar autenticação multifator (MFA) em todos os acessos, tanto para colaboradores quanto para terceiros, além de ampliar o uso de soluções de **Zero Trust**: sempre verificar a identificação.
2. **Aprimoramento nos Treinamentos em Segurança**:
    - **Problema**: A baixa adesão cultural à segurança da informação entre os colaboradores foi identificada como uma vulnerabilidade.
    - **Solução Proposta**: Tornar os treinamentos mais frequentes e gamificados, com metas e recompensas para melhorar o engajamento. Promover campanhas mensais de conscientização sobre cibersegurança, focando em novas ameaças.
3. **Automatização do Monitoramento de Ameaças**:
    - **Problema**: O monitoramento depende de ações manuais que podem retardar respostas a ameaças críticas.
    - **Solução Proposta**: Automatizar a resposta a incidentes através da implementação de **SOAR (Security Orchestration, Automation, and Response)**, que integrará o CrowdStrike e o Rapid7, permitindo a detecção automática e a resposta imediata a ameaças.
4. **Gestão de Shadow IT**:
    - **Problema**: A prática de Shadow IT, onde os colaboradores usam softwares não autorizados, é uma das principais fontes de vulnerabilidade.
    - **Solução Proposta**: Implementar políticas rígidas de bloqueio e monitoramento contínuo de atividades de rede, além de fortalecer o uso do **ClearPass** para controlar e bloquear acessos não autorizados. Treinamentos específicos para conscientizar os colaboradores sobre os riscos de utilizar softwares não autorizados também são recomendados.
5. **Melhoria no Controle de Acesso Físico**:

- **Problema**: O controle de acesso físico a áreas críticas da empresa pode ser comprometido por práticas inadequadas.
- **Solução Proposta**: Implementar sistemas de controle de acesso por biometria ou senha e cartões de identificação para todas as áreas sensíveis, além de melhorar o monitoramento por câmeras.

4.3. Conclusão

Essas melhorias vão ajudar a Real Moto Peças a reduzir os riscos de segurança da informação e promover uma cultura de segurança entre os funcionários.

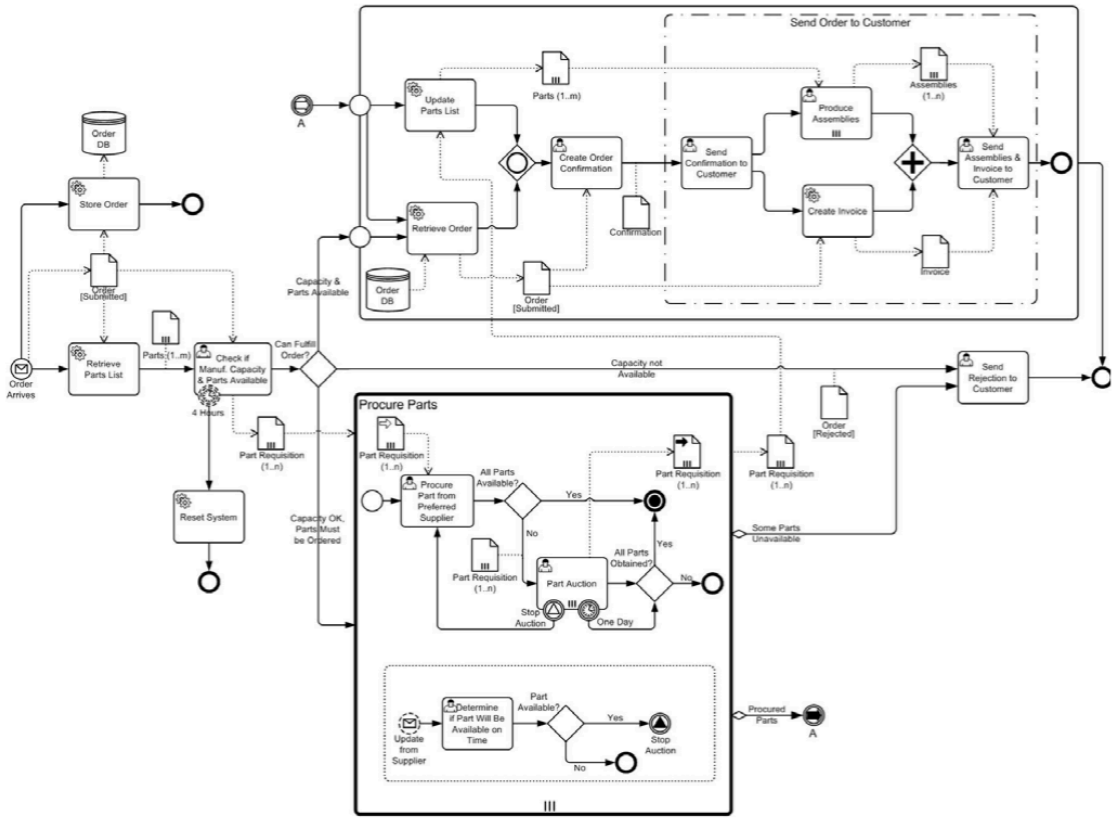


Figure 7.8 – An example of a stand-alone Process (Orchestration) diagram

Fonte: OMG, 2014 p.45

Disponível em: OMG. Object Management Group. Business Process Model and Notation (Links para um site externo.). v. 2.0.2. Jan 2014.

AVALIAÇÃO DAS NORMAS DE SEGURANÇA DA EMPRESA

Acesso físico

Implementamos medidas que protegem as instalações físicas onde o sistema de SI e os recursos de TI estão localizados. São estabelecidas medidas de controle de acesso, que impedem acessos não autorizados em áreas críticas, tais como:

- Uso de crachás;
- Portaria;
- Biometria
- Biometria cadastrada (para acesso a setores de infraestrutura de segurança);
- Sistema de câmeras (principalmente no setor de estoque) e 5 DVRs;
- Nobreak (sustentação de 4 horas);
- Brigada de incêndio.

Estações de trabalho

As estações de trabalho são acessadas apenas por funcionários com credenciais de acesso válidas, o logoff é obrigatório sempre que as estações de trabalho não estiverem em uso. Caso o funcionário precise se ausentar temporariamente de sua estação, o bloqueio de tela deve ser feito. A estação de trabalho deve ser usada estritamente no horário de expediente e apenas para fins de trabalho. A área de trabalho deve estar sempre limpa e organizada, evitando acúmulo de documentos sensíveis e confidenciais nas estações.

Impressora

O uso das impressoras é somente com acesso autorizado, utilizadas somente de forma responsável e eficiente para o trabalho. Documentos confidenciais são impressos somente em casos de necessidade. O descarte de documentos sensíveis deve ser feito por meio de triturador de papel ou serviços de destruição de documentos.

Dispositivos pessoais (Shadow IT)

Vendedores utilizam aparelhos móveis próprios para trabalhar. O número de WhatsApp é fornecido pela empresa junto à Embratel. Há um problema ainda sem solução para ex-vendedores que continuam usando o número da empresa.

Já nos equipamentos usados por diretores e supervisores é usada ferramenta de autenticação multifatorial (MFA). Alguns desses colaboradores usam ainda ferramenta de VPN no celular para acessar recursos específicos.

Atualização de softwares

As atualizações são realizadas por um programa central e também via acesso remoto. Esse acesso permite também desinstalações em massa e o acionamento de equipamentos.

Testes de segurança

Uma empresa terceirizada é contratada regularmente para a realização de testes de invasão ao site, servidores e VPN da Real Moto Peças. O relatório é acessível apenas a diretores e gerentes.

- Relatar sobre a análise de riscos, plano de contingência e normas técnicas aplicadas.
    1.

Exemplo:

Tipo de controle	**Descrição**	**Responsável**
Sistema Sênior	Registro de dados relativos aos colaboradores da empresa.	RH
CrowdStrike	Monitoramento de ameaças internas e externas	TI
Treinamento	Treinamento de funcionários e colaboradores.	TI
Logoff	Usuários devem realizar o logoff das estações de trabalho sempre que não estiverem presentes.	Todos

Manipulação de dados	Usuários devem levar em conta na manipulação e tratamento de dados as diretrizes determinadas na LGPD.	De acordo com nível de acesso

Análise de risco:

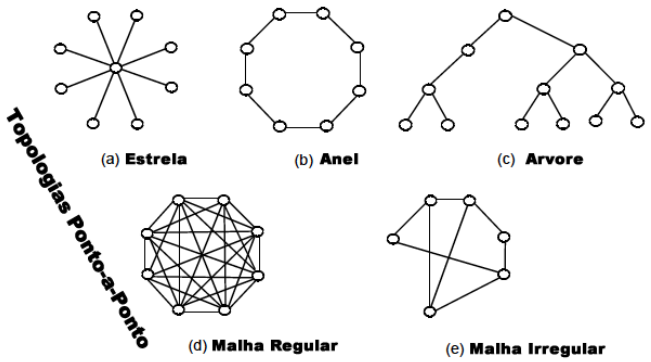
Tipo de exposição	**Probabilidade de ocorrência**	**Estimativa de prejuízo (mensal/anual)**
Sistema Sênior - Registro equivocado de dados	Alta	Insignificante
CrowdStrike - Não atualização (ransomware)	Rara	Até US$ 1,85 milhão
Phishing (violação de dados)	Baixa	U$ 4,5 milhões
Uso de telefone da empresa por ex-funcionários	Alta	Perda de clientes
Danos imagem corporativa	Variável	Incalculável
Violações a LGPD	Média	Até 2% do faturamento

6. TOPOLOGIA DE REDE (Etapa 3)

Discorra sobre como os computadores e outros componentes estão conectados em uma rede de computadores.

- Identificar e desenhar a topologia de rede da organização.

Barramento / estrela / barra / anel



Disponível em: https://tsilvestre.wordpress.com/redes/redes-ponto-a-ponto-e-difusao-topologias/ acesso em 10/11/2021.

- Identificar os tipos de redes utilizados pela organização.

Exemplo:

- PAN (Personal Area Network);
- WPAN (Wireless Personal Area Network);
- LAN (Local Area Network);
- WLAN (Wireless Local Area Network);
- MAN (Metropolitan Area Network);
- WAN (Wide Area Network);
- Redes Interconectadas (Internet).
    - Traga informações sobre os sinais da rede: analógico, digital/ meios de transmissão: Guiados(fio), não guiado (sem fio). Dentre outras informações relevantes.
    - Aqui, demonstre também o processo de planejamento, desenvolvimento e avaliação do projeto que estão desenvolvendo. Fale sobre a metodologia, ferramentas que estão sendo utilizadas).
    - Demonstrem imagens ilustrativas.
    - Identifique as principais normas e padrões com foco em segurança da informação
    - Processos de auditoria
    - Certificações

7. Aplicação de tecnologias de informação e comunicação (Etapa 4)

Discorra sobre os impactos das tecnologias de informação e comunicação na sociedade, estruturas e processos organizacionais, bem como os aspectos éticos e legais relacionados à segurança da informação aplicados pela empresa. Como a empresa adota, enxerga e dissemina essa cultura. Como as pessoas são incluídas digitalmente na organização. Como é estabelecida a relação entre as pessoas.

REFERÊNCIAS (Etapa 4)

Cite os autores mencionados no texto.

APÊNDICES (Documentos produzidos pelos autores) (Etapa 4)

Plano de Pesquisa

1.PROBLEMA DE PESQUISA

2.PÚBLICO ALVO

3.DETERMINAÇÃO DOS OBJETIVOS

4.METODOLOGIA

4.1 Tipo de Pesquisa

4.2 **Método da pesquisa**

4.3 Técnicas de coleta de dados

5. UNIVERSO E AMOSTRA

6. INSTRUMENTOS DE COLETA DE DADOS

7. RESULTADOS DA PESQUISA

7.1 Dados da pesquisa quantitativa

Colocar todas as questões representadas em quadros, tabelas e gráficos

7.2 Dados da pesquisa qualitativa –

7.3 Dados da pesquisa qualitativa –

8.CONCLUSÕES

Aponte os principais resultados das pesquisas

ANEXOS

Anexe os documentos utilizados no trabalho.