# Projeto A3 - Sistemas Computacionais e Segurança
# Solidum Seguros

## Breve descrição da empresa:

Somos a Solidum Seguros, uma empresa especializada em seguros em diversas áreas como vida, imóveis e automóveis. Além disso, nossa equipe com mais de 100 funcionários está sempre a postos para a resolução de qualquer problema. A empresa possui 171 funcionários. As principais tarefas/informações/produtos da empresa são coberturas de seguro que abrangem diversos eventos como acidente com veículos, imóveis e vida.

## Áreas existentes:

**1 - Área de emissão de apólice:**

Área onde é assinado e emitido o documento que formaliza a aceitação de risco objeto do contrato do seguro. Essa área possui 20 funcionários.

**2 - Área comercial (parcerias, corretores, clientes e marketing):**

Área para a efetivação de parcerias com outras empresas, corretores e emissão de novos seguros para novos clientes. Além, claro, da área de marketing para propagandas. Essa área possui 40 funcionários.

**3 - Área de sinistro:**

Área onde possuem os atendentes que atendem o segurado no momento do acidente e os técnicos que fazem o relatório completo do acidente e análise de cobertura. Essa área possui 50 atendentes e 20 técnicos.

**4 - Área de tecnologia:**

Área responsável pela manipulação dos softwares ERP (planejamento de recursos empresariais), manutenção dos sites da empresa e possíveis integrações com outras empresas. Essa área possui 25 funcionários.

**5 - Área financeira:**

Área responsável pelo controle financeiro da empresa. Essa área possui 10 funcionários.

**6 - Área de RH (direção, coordenação, analista e assistentes):**

Área responsável pelas contratações e desligamentos de funcionários e estagiários, além de manter uma boa comunicação entre os funcionários e os objetivos da empresa. Essa área possui 6 funcionários.

## Softwares necessários:

- ➔ Opera - Navegador principal para o sistema;
- ➔ Pacote Office - Word, Excel, PowerPoint e Teams;
- ➔ WhatsApp - Meio de comunicação mais dinâmico;
- ➔ Guidewire - Software dedicado para o ramo de seguros;
- ➔ Digibee - Integração de serviços com parceiros.

## Equipamentos utilizados:

- ➔ Notebooks:

  Lenovo Ultrafino IdeaPad 3:
  - Quantidade: 60 unidades;
  - Processador: AMD Ryzen 7 5700U;
  - Memória RAM: 8 GB DDR4 3200 MHz expansível até 16 GB;
  - Armazenamento: 512 GB de SSD;
  - Valor: R$ 3.300,00;
  - Será utilizado pelos funcionários da área de tecnologia e financeira e pelos técnicos da área de sinistro.

  Lenovo Ultrafino IdeaPad 1:
  - Quantidade: 120 unidades;
  - Processador: AMD Ryzen 5 7520U;
  - Memória RAM: 8 GB DDR4 3200 MHz expansível até 16 GB;
  - Armazenamento: 256 GB SSD;
  - Valor: R$ 2.900,00;
  - Será utilizado pelos demais funcionários.

- ➔ Hardware:

  Roteador Cisco ISR 1100 Series:
  - Quantidade: 1 unidade;
  - Valor: R$ 4.300,00.

Switch Cisco SG220-26:

- Quantidade: 3 unidades;
- Valor: R$ 1.900,00 (cada).

Firewall Fortinet FortiGate 60E + Licença UTP 24 meses:

- Quantidade: 1 unidade;
- Valor: R$ 4.900,00.

Access Point Cisco Business CBW240AC-Z:

- Quantidade: 5 pontos;
- Valor: R$ 1.500,00 (cada).

Servidor NAS Synology DS923+:

- Quantidade: 1 unidade;
- Valor: R$ 6.100,00.

Servidor Dell T320:

- Quantidade: 2 unidades;
- Valor R$ 4.500,00 (cada).

Nobreak Apc Back-UPS:

- Quantidade: 2 unidades;
- Valor: R$ 1.200,00 (cada).

Cabo De Rede Cat6 50 Metros:

- Quantidade: 10 unidades;
- Valor: R$ 60,00 (cada).

Conector Fortrek Rj45 Macho Cat5e (pacote com 100):

- Quantidade: 2 unidades;
- Valor: R$ 40,00 (cada).

Patch Panel 24 Portas Cat6 - WT-2178C-110-24P:

- Quantidade: 5 unidades;
- Valor: R$ 120,00 (cada).

➔ Sistema Operacional e Softwares:
Todos os notebooks possuem o sistema operacional Windows 11. Os softwares a serem utilizados serão Opera, todo o pacote Office, WhatsApp, Guidewire e Digibee.

## Análise de Vulnerabilidade e Plano de Segurança:

Todos os funcionários deverão seguir o sistema IAM (método de identificação de acesso) e possuir um login único com senha própria para gerenciar o controle de acesso dos usuários no sistema (se necessário, será implementado um sistema de identificação biométrica). Também, haverão normas de segurança interna (PSI) para regular e advertir/penalizar qualquer infração. Além disso, a empresa seguirá de acordo com a Lei Geral de Proteção de Dados (LGPD). Outras boas práticas são: manter os sistemas operacionais atualizados, realizar backups com a frequência necessária (diário, semanal ou mensal), seguir os três pilares fundamentais do modelo clássico de segurança (CID) e as normas ISO e IEC.

As boas práticas dos funcionários em uma empresa de seguros incluem a proteção de dados do cliente, treinamento em segurança de dados, acesso controlado a informações, educação sobre phishing e uso responsável da tecnologia, além de manter atualizações de software, senhas fortes e relatórios éticos. Eles também devem estar atentos à segurança física das instalações, à prevenção de fraudes e à colaboração com a equipe de segurança, enquanto seguem as políticas de segurança de documentos e treinamentos de conformidade, contribuindo assim para a proteção de informações confidenciais e a conformidade com as regulamentações do setor de seguros.

| Item | Risco | Impacto | Probabilidade | Consequências | Resposta |
|---|---|---|---|---|---|
| 1 | Fraude de sinistros. | Alto. | Médio. | Perdas financeiras significativas, reputação danificada. | Implementação de procedimentos rigorosos de verificação de sinistros, análise de dados para detecção de fraudes. |
| 2 | Risco de investimento. | Alto. | Médio. | Perdas financeiras devido a investimentos arriscados. | Diversificação de investimentos, análise de risco, consultoria financeira. |
| 3 | Ciberataques e violação de dados. | Alto. | Médio. | Roubo de informações sensíveis e penalidades legais. | Fortalecimento da segurança de TI, treinamento em segurança cibernética, protocolos de resposta a incidentes. |
| 4 | Concorrência acirrada no mercado. | Médio. | Médio. | Perda de participação de mercado. | Estratégias de marketing, desenvolvimento de produtos, diferenciação de serviços. |

| | | | | | |
|---|---|---|---|---|---|
| 5 | Mudanças na regulamentação. | Médio. | Médio. | Requisitos regulatórios adicionais e custos. | Acompanhamento regulatório, ajuste de políticas e procedimentos, conformidade. |
| 6 | Catástrofes naturais. | Alto. | Baixo. | Grandes perdas devido a desastres naturais. | Reavaliação de políticas de seguro, gestão de risco de catástrofes. |
| 7 | Mudanças nas taxas de juros. | Médio. | Médio. | Impacto nas receitas de investimento. | Acompanhamento econômico, estratégias de gestão de ativos. |
| 8 | Envelhecimento da carteira de segurados. | Médio. | Médio. | Maior risco de sinistros e necessidades médicas. | Desenvolvimento de produtos para atender a diferentes faixas etárias, análise de políticas. |
| 9 | Mudanças demográficas e sociais. | Médio. | Baixo. | Mudanças nas demandas do mercado e nas necessidades. | Pesquisa de mercado, adaptação de produtos e estratégias de marketing. |
| 10 | Problemas de liquidez. | Alto. | Médio. | Dificuldades financeiras e solvência. | Gerenciamento financeiro prudente, reserva de capital, linhas de crédito de emergência. |

## Proteção contra Ameaças:

**1 - Fraude de Sinistros:**

Implementar sistemas de detecção de fraude avançados que usam análise de dados e aprendizado de máquina para identificar padrões suspeitos. Realizar auditorias regulares em sinistros de alto valor. Promover a educação e conscientização dos segurados sobre a importância da honestidade e transparência na apresentação de sinistros.

**2 - Risco de Investimento:**

Diversificar a carteira de investimentos para reduzir o risco. Contratar especialistas em gestão de investimentos para tomar decisões informadas. Monitorar constantemente o desempenho dos investimentos e ajustar a estratégia conforme necessário.

**3 - Ciberataques e Violação de Dados:**

Investir em segurança cibernética robusta, incluindo firewalls, antivírus e detecção de intrusões. Manter sistemas e software atualizados para corrigir vulnerabilidades conhecidas. Realizar treinamento de conscientização em segurança cibernética para funcionários e terceirizados. Implementar um plano de resposta a incidentes para reagir rapidamente a violações de dados.

**4 - Concorrência Acirrada no Mercado:**

Inovar em produtos e serviços para se destacar no mercado. Realizar análises de mercado regulares para entender as tendências e as necessidades dos clientes. Construir relacionamentos sólidos com os clientes para mantê-los fiéis à empresa.

**5 - Mudanças na Regulamentação:**

Manter uma equipe jurídica atualizada sobre as regulamentações relevantes. Acompanhar ativamente as mudanças regulatórias e se adaptar a elas. Manter um sistema de gestão de conformidade para garantir que a empresa esteja em conformidade com as leis e regulamentações aplicáveis.

**6 - Catástrofes Naturais:**

Diversificar as apólices em diferentes regiões geográficas para reduzir o risco de exposição a catástrofes em uma única área. Manter um plano de contingência para atender rapidamente aos segurados afetados por catástrofes naturais.

**7 - Mudanças nas Taxas de Juros:**

Diversificar a carteira de investimentos para se adaptar a diferentes cenários de taxa de juros. Monitorar de perto as tendências das taxas de juros e fazer ajustes estratégicos quando necessário.

**8 - Envelhecimento da Carteira de Segurados e Mudanças Demográficas e Sociais:**

Desenvolver produtos e serviços adequados às necessidades e preferências de diferentes grupos demográficos. Atualizar constantemente as políticas de subscrição para refletir as mudanças nas condições demográficas e sociais.

**9 - Problemas de Liquidez:**

Manter uma gestão financeira sólida e um planejamento de liquidez adequado. Estabelecer linhas de crédito de emergência para situações de crise. Monitorar de perto os fluxos de caixa e tomar medidas proativas para evitar problemas de liquidez.

## Plano de Contingência:

**Ataques Cibernéticos:**

Cada funcionário da área de tecnologia terá uma função para gerenciar o dano causado:

- 5 serão responsáveis por combater o ataque que está ocorrendo, reportando para o gestor dos avanços e necessidades para o prosseguimento do trabalho;
- 5 ficarão responsáveis por colocar os backups em produção, para que as principais atividades da empresa funcione de maneira adequada;
- 5 irão procurar falhas que tenham contribuído para um ataque em nossos sistemas;
- 5 irão trabalhar em aprimorar nossos sistemas, e acabar com todas as vulnerabilidades do mesmo;
- 5 irão avaliar os danos que todas as áreas de nossa empresa podem ter sofrido e repassar para o gestor da equipe, para que ele tome todas as providências cabíveis e faça um relatório para a equipe jurídica, e então receber uma orientação de como prosseguir em caso de violação de dados ou dados vazados, entre outros riscos.

**Falhas de Equipamentos:**

Em caso de falha em quantidades numerosas de equipamentos, nossos técnicos irão alocar outros equipamentos da empresa em áreas estratégicas visando manter as principais operações da empresa em funcionamento.

Em caso de falha no servidor, realizaremos o acionamento da equipe de resposta a incidentes e a restauração a partir de backups, caso necessário. Após isso, os backups devem ser mantidos constantes e atualizações regulares devem ser fornecidas.

Em caso de quedas de energia, serão ativados os geradores elétricos para continuar os processos e atividades com normalidade. Se a falta de energia permanecer por um longo período, entraremos em contato com nossos clientes e faremos comunicados em nossas redes sociais.

**Desastres Naturais:**

Analisaremos a dimensão e a gravidade do desastre para entender como iremos prosseguir com nosso plano. Também, mobilizaremos nossa equipe de recursos humanos para lidar com o aumento de ligações e reclamações. Nossos 20 técnicos serão designados para termos uma resposta eficiente a todos os chamados. Entraremos em contato imediato com clientes que foram afetados. Estabeleceremos canais de comunicação rápidos e eficazes para tirarmos dúvidas e fornecermos atualizações regulares a todos os clientes. Entraremos em contato com os serviços de emergência e autoridades locais para ficarmos cientes do ocorrido e decidirmos quais medidas cabíveis devemos tomar a partir disso.

**Greves ou Paralisações:**

Em caso de algum desses empecilhos, nossa empresa acionará nossa equipe de contingência para que nossas operações não sejam paralisadas por completo. Comunicaremos a todos nossos clientes sobre o acontecimento e deixaremos claro que teremos nosso contingente reduzido. Tentaremos negociar para que nossos funcionários trabalhem remotamente para manter nossas operações temporariamente.

**Interrupção de Serviços de Telecomunicações:**

Em caso de interrupção, nossa empresa terá conexões de backup e o monitoramento contínuo da rede. Usaremos o plano de contingência para garantir a resiliência da infraestrutura de telecomunicações, minimizando o impacto de possíveis falhas e assegurando a continuidade dos serviços.

## IoT que podem ser implantados:

**1 - Dispositivos de Telemetria em Veículos Segurados:**

Instalação de dispositivos de telemetria em veículos segurados para monitorar o comportamento do motorista, como velocidade, frenagem e aceleração. Isso pode ajudar a avaliar o risco do segurado e oferecer prêmios mais personalizados.

**2 - Sensores de Prevenção de Sinistros:**

Utilização de sensores de IoT em imóveis segurados para detectar condições que podem levar a sinistros, como vazamentos de água, incêndios, inundações e intrusões. Isso pode permitir intervenções proativas e redução de sinistros.

**3 - Dispositivos de Saúde Conectada:**

Parcerias com empresas de dispositivos de saúde conectadas para oferecer seguros de saúde personalizados com base nos dados de saúde coletados por dispositivos como smartwatches e medidores de saúde.

**4 - Monitoramento de Ativos em Tempo Real:**

Utilização de sensores IoT para rastrear ativos valiosos, como obras de arte, joias ou colecionáveis, proporcionando proteção adicional para os segurados.

**5 - Medidores Inteligentes de Utilidades:**

Monitoramento de consumo de energia, água e gás em propriedades seguradas para avaliar riscos e oferecer descontos ou prêmios mais baixos para aqueles que adotam práticas de consumo eficiente.

**6 - Sistemas de Segurança Doméstica Conectada:**

Parcerias com fornecedores de sistemas de segurança residencial conectada para oferecer seguros que integrem sistemas de vigilância por vídeo, detecção de intrusão e monitoramento em tempo real.

**7 - Análise de Dados Avançada:**

Coleta e análise de dados de dispositivos IoT para identificar tendências e padrões que podem aprimorar a avaliação de riscos, a subscrição de apólices e a detecção de fraudes.

**8 - Gestão de Frota de Veículos Comerciais:**

Monitoramento em tempo real da frota de veículos de clientes empresariais para melhorar a segurança, a manutenção preventiva e a otimização de rotas.

**9 - Sensores Ambientais:**

Utilização de sensores ambientais para monitorar condições climáticas e geográficas que possam impactar o risco de eventos como inundações, incêndios ou desastres naturais.

**10 - Conectividade do Cliente:**

Fornecimento de aplicativos e dispositivos IoT para os clientes acessarem informações de apólices, pagar prêmios e relatar sinistros de maneira conveniente.

**11 - Sensores de Saúde em Seguros de Vida:**

Uso de dispositivos de IoT para coletar dados de saúde dos segurados, como frequência cardíaca, atividade física e hábitos alimentares, para ajustar as taxas de apólice com base no estilo de vida.

## Utilização de Cloud:

**1 - Benefícios:**

➔ Escalabilidade:
- A nuvem permite escalar recursos de acordo com a demanda, garantindo que a plataforma possa lidar com picos de tráfego durante eventos especiais ou situações de alta demanda.

➔ Acesso Remoto:
- A equipe pode acessar dados e sistemas a qualquer momento e de qualquer lugar, facilitando o trabalho remoto e melhorando a eficiência operacional.

➔ Agilidade no Desenvolvimento:
- Ambientes de nuvem oferecem ferramentas e serviços que facilitam o desenvolvimento, acelerando o ciclo de vida do software.

➔ Redução de Custos de Infraestrutura:
- Evita a necessidade de investir em hardware próprio, reduzindo os custos iniciais e permitindo que a empresa pague apenas pelos recursos utilizados.

➔ Backup e Recuperação:

- Serviços de nuvem geralmente incluem soluções automáticas de backup e recuperação, garantindo a integridade dos dados.

**2 - Considerações:**

➔ Segurança:
- A segurança dos dados é uma preocupação crítica. É necessário implementar práticas robustas de segurança, como criptografia, controle de acesso e monitoramento constante.

➔ Conformidade Regulatória:
- Empresas de seguros frequentemente lidam com informações sensíveis. Garantir a conformidade com regulamentações, como GDPR ou normas específicas do setor, é essencial.

➔ Custos Variáveis:
- Embora a nuvem ofereça flexibilidade, os custos podem variar com o consumo de recursos. É vital gerenciar cuidadosamente os gastos para evitar surpresas financeiras.

➔ Dependência de Provedores:
- Ao optar por serviços de nuvem, a empresa se torna dependente do provedor. Uma mudança pode ser desafiadora e pode exigir migração de dados.

➔ Integração de Sistemas:
- Integrar sistemas existentes com soluções em nuvem pode ser complexo. Planejar uma estratégia eficaz de integração é fundamental.

**3 - Valores (Estimativa):**

➔ Armazenamento em Nuvem (por 5 TB): $100 a $150 por mês;
➔ Máquinas Virtuais (IaaS): $300 a $1,000 por mês;
➔ Banco de Dados Gerenciado: $100 a $300 por mês por instância;
➔ Serviços de Rede e Tráfego: $100 a $200 por mês;
➔ Serviços Adicionais (monitoramento, segurança): $50 a $200 por mês.

Total Estimado: $650 a $1,850 por mês.