Universidade Pontifícia Católica de Minas Gerais (PUC Minas)

Curso: Segurança da Informação

Disciplina: Projeto: Fundamentos de Sistemas

Proposta de Soluções Seguras

Equipe de Trabalho

Alexandre Zacura Luiz 877868

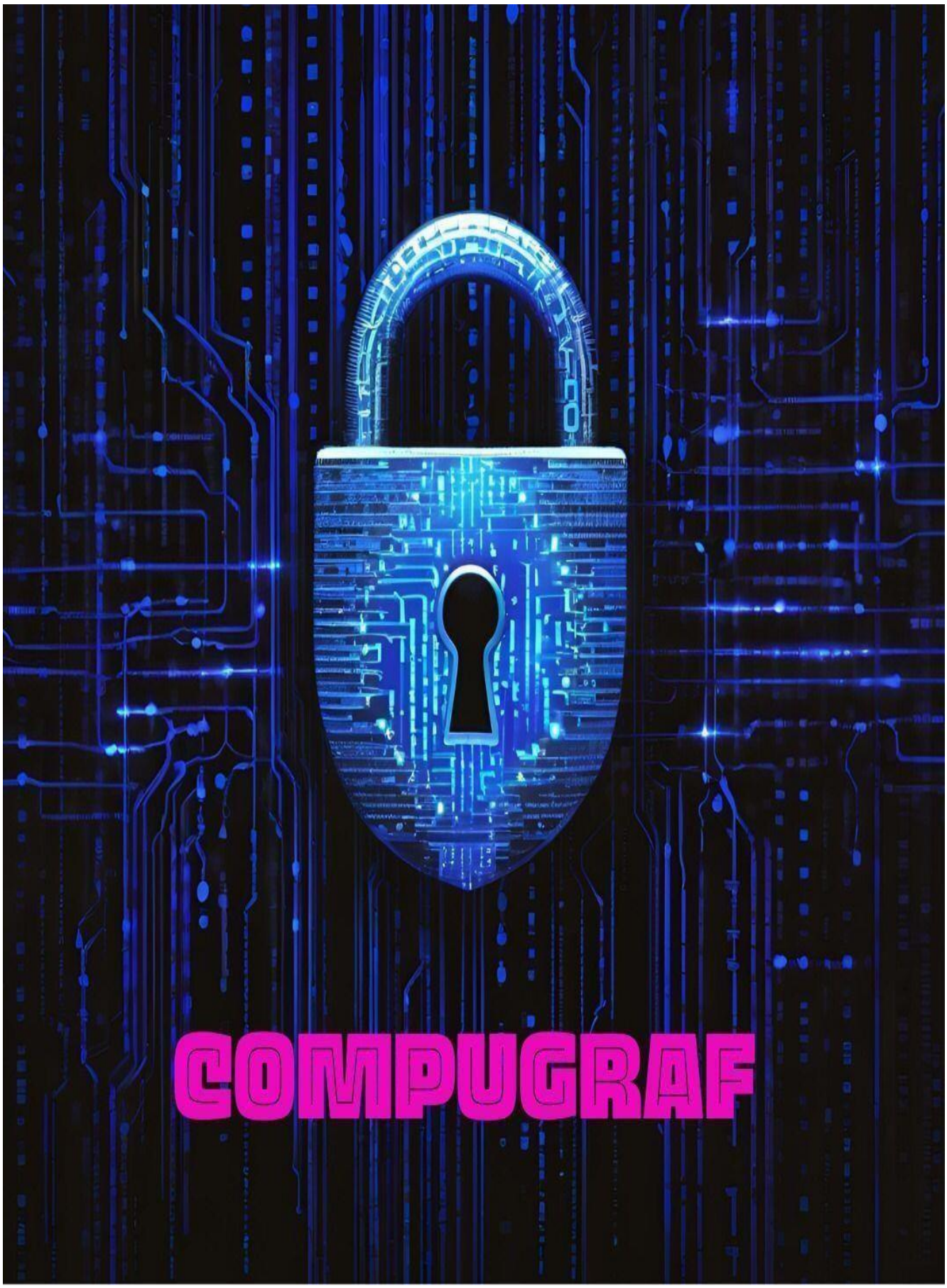
Marcio de Souza Braga 875364

Pedro Manoel 877798

Yasmin da Silva Martins Siqueira 874756

Orientador

Pedro Ivo Alexandre de Oliveira


COMPUGRAF

Sumário

1. INTRODUÇÃO

As empresas enfrentam ameaças cibernéticas vastas e multifacetadas, como malware, ataques de phishing e exposição de dados, que evoluem rapidamente, tornando a proteção eficaz dos sistemas cada vez mais desafiadora. Nesse cenário, a Compugraf, uma empresa especializada em cibersegurança, destaca-se por oferecer serviços que ajudam seus clientes a desenvolver seus negócios e superar os desafios da transformação digital.

1.2. Apresentação da Empresa Compugraf

Nascemos há mais de 41 anos e ajudamos a moldar o cenário tecnológico ao longo de gerações, atuando com inteligência no combate às ameaças cibernéticas. Contamos com profissionais altamente qualificados para apoiar empresas nos desafios da segurança digital. Somos uma empresa brasileira cuja história começou em 1982, no mercado de computação gráfica. Nos anos 1990, a proliferação da internet trouxe grandes desafios de segurança para as empresas, e nosso propósito passou a ser protegê-las com soluções de ponta em cibersegurança. Fomos pioneiros ao firmar parcerias com grandes fabricantes mundiais, como a Check Point, trazendo a cibersegurança para o Brasil. Com uma abordagem personalizada e centrada no cliente, nos orgulhamos de ser referência no mercado de cibersegurança, reconhecidos por nossa excelência, confiabilidade e compromisso com a inovação.

Etapa 1

CONHECIMENTO DA LEGISLAÇÃO DE SEGURANÇA DA INFORMAÇÃO

2. Compreendendo a organização

Compugraf é uma empresa brasileira especializada em cibersegurança, com mais de 40 anos de experiência no mercado, oferecendo uma gama de soluções e serviços voltados à proteção de dados, infraestruturas digitais e conformidade regulatória.

2.2 O negócio

A companhia se destaca no desenvolvimento de soluções integradas que vão desde proteção de redes e dados até a segurança em ambientes de computação em nuvem, além de contar com parcerias estratégicas com grandes players de tecnologia**.**

3 Os principais processos de negócios

- Avaliação e Análise de Vulnerabilidades;
- Desenvolvimento de Soluções Customizadas;
- Implementação de Soluções;
- Monitoramento Contínuo e Gerenciamento de Segurança;
- Resposta a Incidentes;
- Atualização e Patch Management;
- Gestão de Conformidade e Políticas de Segurança;
- Treinamento e Capacitação de Usuários;
- Revisão e Otimização Contínua;
- Suporte Técnico e Atendimento ao Cliente

Dentro destes grupos temos os seguintes detalhamentos:

- Avaliação e Análise de Vulnerabilidades:

  - Realiza auditorias de segurança e testes de penetração para identificar vulnerabilidades e mapear pontos fracos da infraestrutura digital, criando um plano de mitigação para resolvê-los.

- Desenvolvimento de Soluções Customizadas

  -Com base nas análises, a Compugraf desenvolve soluções personalizadas de cibersegurança, integrando tecnologias adequadas às necessidades específicas do cliente.

- Implementação de Soluções:

  - Após a definição das tecnologias, a empresa implementa e configura firewalls, DLPs, EDRs e outras ferramentas, garantindo que a infraestrutura digital esteja protegida e funcionando conforme o esperado.

- Monitoramento Contínuo e Gerenciamento de Segurança:

  - A Compugraf oferece monitoramento em tempo real e gerenciamento contínuo

das redes dos clientes, utilizando soluções como SIEM e MSSP para identificar e responder rapidamente a ameaças.

- Resposta a Incidentes

- Quando ocorre uma ameaça, a Compugraf reage rapidamente, identificando, contendo e eliminando o ataque, além de restaurar sistemas e realizar análises pós-incidente.

- Atualização e Patch Management

  - A Compugraf gerencia a aplicação de atualizações e patches de segurança, assegurando que as soluções usadas estejam protegidas contra vulnerabilidades recém-descobertas.

- Gestão de Conformidade e Políticas de Segurança:

  - A empresa ajuda clientes a cumprir requisitos legais e regulamentares, implementando políticas de segurança e monitorando a conformidade contínua com normas de proteção de dados.

- Treinamento e Capacitação de Usuários:

  - A Compugraf oferece treinamentos para aumentar a conscientização sobre cibersegurança, como reconhecer tentativas de phishing e aplicar práticas seguras no uso de sistemas e dados.

- Revisão e Otimização Contínua:

  - A empresa revisa regularmente as soluções implementadas, ajustando políticas de segurança e sugerindo atualizações para lidar com novas ameaças ou necessidades emergentes.

- Suporte Técnico e Atendimento ao Cliente:

  - A Compugraf disponibiliza suporte técnico 24/7 para solucionar problemas operacionais e técnicos, além de prestar assistência em casos de incidentes de segurança mais graves.

  - **Obs.:** Esses processos garantem que a Compugraf ofereça uma proteção abrangente e contínua para seus clientes, desde a análise inicial até a resposta a incidentes e o suporte técnico.

2. 1 Leis relacionadas a TI que impactam o negócio

Tabela 1- Leis relacionadas à TI

Lei	**Impacto na organização**

LGPD	**Bases Legais para o Tratamento de Dados :** A Compugraf deve garantir que o tratamento de dados pessoais seja feito com base em uma das bases legais da LGPD, como consentimento ou legítimo interesse. **Segurança e Proteção de Dados :** A empresa deve adotar medidas técnicas e organizacionais para proteger os dados pessoais contra acessos não autorizados, incidentes de segurança e vazamentos. **Responsabilidade como Controladora ou Operadora :** A Compugraf deve garantir conformidade tanto como controladora quanto como operadora de dados, sendo responsável por como os dados são coletados, armazenados e utilizados. **Direitos dos Titulares de Dados :** A empresa precisa estar preparada para atender solicitações dos titulares, como acesso, correção ou exclusão de dados pessoais. **Notificação de Incidentes :** Em caso de vazamentos ou incidentes de segurança, a Compugraf deve notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares de dados afetados. **Relatório de Impacto à Proteção de Dados :** Para operações de tratamento que envolvam riscos elevados, a empresa pode ser solicitada a elaborar um relatório detalhado avaliando esses riscos e as medidas de mitigação. **Multas e Sanções :** A não conformidade pode resultar em multas de até 2% do faturamento anual, limitadas a R$ 50 milhões por infração, além de advertências ou bloqueios de tratamento de dados.
Marco Civil	**Neutralidade da Rede :** A Compugraf deve assegurar que os dados trafeguem na internet sem discriminação ou priorização de conteúdo, garantindo a neutralidade da rede em suas soluções de conectividade. **Proteção de Dados Pessoais :** A empresa deve seguir regras rigorosas sobre coleta, armazenamento e tratamento de dados pessoais, garantindo a privacidade e segurança dos usuários, em linha com a LGPD. **Retenção de Registros de Conexão :** Se a Compugraf armazenar registros de conexão e navegação, deve mantê-los sob sigilo por, no máximo, 12 meses e só divulgá-los mediante ordem judicial.

	Responsabilidade por Conteúdos de Terceiros : A empresa não é responsável por conteúdos postados por terceiros, a menos que, após ordem judicial, não remova conteúdos considerados ilícitos. **Garantia de Liberdade de Expressão :** A Compugraf deve garantir que suas plataformas e serviços não comprometam a liberdade de expressão dos usuários, respeitando os princípios de livre acesso à internet. **Segurança da Informação :** A empresa é responsável por implementar medidas de segurança adequadas para proteger a integridade dos dados e sistemas que administra ou oferece como serviço.

Fonte: LEI Nº 12.965, DE 23 DE ABRIL DE 2014, Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709

Matriz de relacionamento de processos organizacionais e leis.

Tabela 2- Matriz de relacionamento

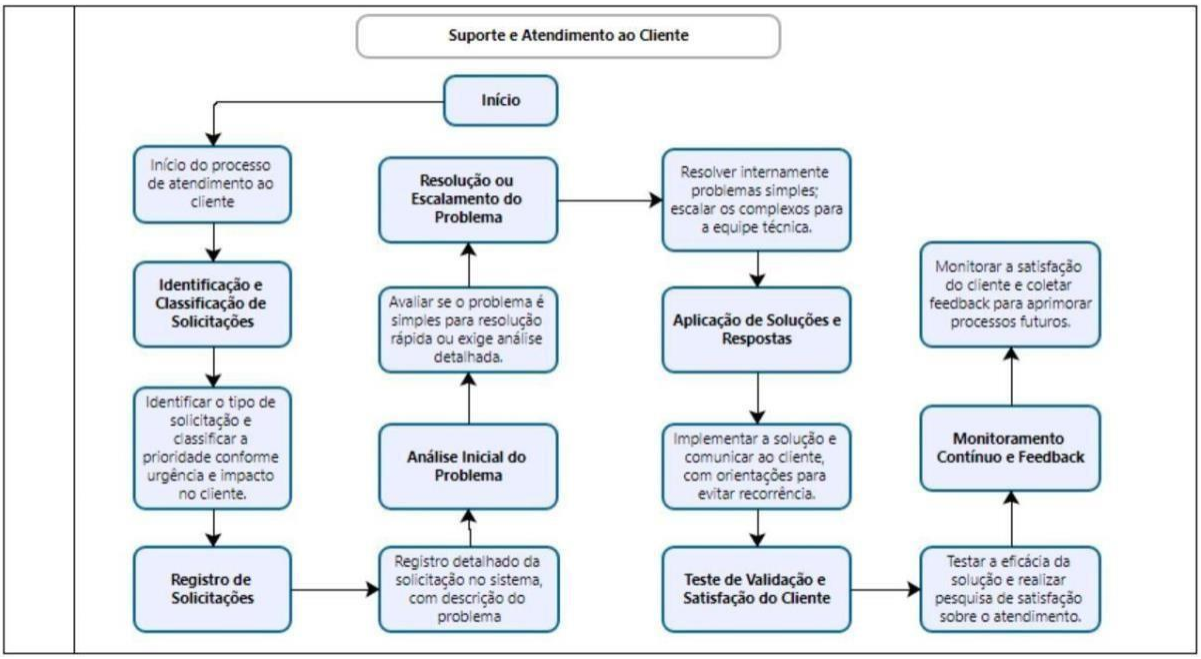
Processo	Leis a serem observadas

Gerenciamento de relacionamento de cliente	**Lei Geral de Proteção de Dados (LGPD)**. A LGPD (Lei nº 13.709/2018) estabelece regras para o tratamento de dados pessoais, incluindo dados sensíveis, que requerem proteção adicional. **Regulamento Geral sobre a Proteção de Dados (RGPD).** O RGPD (Regulamento (UE) 2016/679) regula o tratamento de dados pessoais na União Europeia e também abrange dados sensíveis. **Código de Defesa do Consumidor (CDC)**. A Lei nº 8.078/1990 protege os direitos dos consumidores no Brasil. **Marco Civil da Internet:** A Lei nº 12.965/2014 estabelece princípios e diretrizes para o uso da internet no Brasil. **Setor Financeiro**: Instruções do Banco Central e regras da Lei nº 12.414/2011 sobre proteção de dados de clientes.
Treinamento e capacitação do usuário	**LGPD**: Lei geral de proteção de dados **CDC**: Código de Defesa do Consumidor **Lei de Direto Autorais número**: 9610/1998 **CLT** -Decreto Lei n 5452/1943 **Normas ISO** 27001 e 900, ISO/IEC 19770, ISO/IEC 20000 **Marco Civil da Internet** Normas de Segurança do Trabalho (NR), caso os treinamentos sejam em ambientes físicos **Lei do Estágio**- n11788/2008 e Regulamentação do Procon e Atendimento ao Consumidor, isso quando o treinamento é oferecido como pós- venda ou de suporte técnico. Essas leis ajudam a garantir que os treinamentos e capacitações, sejam seguros, éticos, eficazes e em conformidade com a regulação vigente.

Suporte Técnico e Atendimento ao Cliente	**Lei Geral de Proteção de Dados (LGPD).** Lei nº 13.709/2018. A LGPD regula o tratamento de dados pessoais, estabelecendo princípios e regras para a coleta, armazenamento, tratamento e compartilhamento de dados de clientes e usuários. O suporte técnico precisa garantir que os dados pessoais tratados sejam protegidos, respeitando o consentimento, finalidades específicas, e os direitos dos titulares de dados. **Código de Defesa do Consumidor** (CDC). A Lei nº 8.078/1990 protege os direitos dos consumidores no Brasil. O CDC é crucial para garantir que o atendimento ao cliente respeite os direitos básicos dos consumidores, como informações claras, proteção contra práticas abusivas, e o direito à reparação de danos. O suporte técnico deve garantir que os serviços sejam prestados de maneira eficiente e transparente, e que as soluções oferecidas aos consumidores estejam dentro do prazo e das condições estabelecidas. **Marco Civil da Internet**: A Lei nº 12.965/2014 estabelece princípios e diretrizes para o uso da internet no Brasil.

1. Escolher 1 processo de negócio entre os que foram identificados na etapa 1 e detalhá- lo usando uma ferramenta de construção de fluxograma.

Fonte: Elaborado pelo autor


Suporte e Atendimento ao Cliente
Início
Início do processo de atendimento ao cliente
Identificação e Classificação de Solicitações
Identificar o tipo de solicitação e classificar a prioridade conforme urgência e impacto no cliente.
Registro de Solicitações
Registro detalhado da solicitação no sistema, com descrição do problema
Análise Inicial do Problema
Avaliar se o problema é simples para resolução rápida ou exige análise detalhada.
Resolução ou Escalamento do Problema
Resolver internamente problemas simples; escalar os complexos para a equipe técnica.
Aplicação de Soluções e Respostas
Implementar a solução e comunicar ao cliente, com orientações para evitar recorrência.
Teste de Validação e Satisfação do Cliente
Testar a eficácia da solução e realizar pesquisa de satisfação sobre o atendimento.
Monitoramento Contínuo e Feedback
Monitorar a satisfação do cliente e coletar feedback para aprimorar processos futuros.

6. **Identificar os componentes suscetíveis a eventos de segurança da informação que fazem parte do processo de negócio escolhido vistos no MF de Fundamentos de Segurança.**

- 1.Infraestrutura de Tecnologia da Informação (TI);
- 2.Sistemas de Informação;
- 3.Aplicações Web e Serviços Online;
- 4.Dados e Informações Sensíveis;
- 5.Colaboradores e Processos Humanos;
- 6.Dispositivos de Usuários;
- 7.Comunicação e Redes de Colaboração;
- 8.Processos de Gestão de Segurança;
- 9.Políticas de Segurança e Conformidade;
- 10.Segurança Física.

7. **Mapear itens relacionados à TI invisível na organização.**

Tabela 3- TI Invisível na Organização

Setor	Item de TI não catalogado	Proprietário	Usuários	Risco	Obs.
RH	Ferramenta de videoconferência não licenciada	Ana Souza	Equipe de RH	Falta de compliance com LGPD	Potencial captura de dados confidenciais
TI	Software de gestão de senhas	João Silva	Equipe de TI	Acesso não monitorado a credenciais	Software com senhas à todas as credenciais. Perigo de movimentação lateral

8. **Identificar dispositivos pessoais utilizados na organização.**

Tabela 4- Dispositivos pessoais utilizados na organização

Setor	Dispositivo	Proprietário	Usuários	Risco	Obs.
Marketing	Smartphone pessoal	Carlos Oliveira	Carlos Oliveira	Comunicação externa não monitorada	Uso de aplicativos terceiros

Vendas	Notebook pessoal	Paulo Santos	Paulo Santos	Falta de backup,perda ou roubo do equipamento, atualizações constantes de software e firewall desativado.	Potencial vazamento de dados de preço e margem de lucro.

9. Identificar riscos de segurança física e lógica discutidos no MF de Fundamentos de Segurança da Informação e encontrados no contexto organizacional estudado.

Tabela 5: Riscos de Segurança física e lógicas

Ativo	Ameaça	Vulnerabilidade
Servidores	Acesso físico não autorizado	Falta de controle de acesso adequado
Dados de clientes	Ataques cibernéticos	Falhas na gestão de acessos e autenticação
Dispositivos móveis	Roubo ou perda de dispositivos	Ausência de criptografia em dados móveis
Banco de dados	Roubo ou perda de dados	Falha de criptografia e backup inadequado
Sistemas de software	Exploração de vulnerabilidades	Software desatualizado ou não corrigido
Equipamentos de rede (roteadores, interruptores)	Invasão e comprometimento	Configurações padrão não alteradas, firmware desatualizado

10. Elaborar uma Política de Segurança da informação para a organização

estudada e baseada em modelo disponibilizado em material de apoio da etapa 2.
Política de Segurança da Informação (PSI) – Compugraf

1. Diagnóstico: Proteção de dados estratégicos, informações de clientes, propriedade intelectual e documentos financeiros.

2. Classificação:

- **Confidenciais: Projetos e informações críticas.**
- **Restritas: Dados internos (financeiros e RH).**
- **Públicas: Materiais divulgados externamente.**

3. Acesso:

- **Executivos: Acesso total.**
- **Gestores: Acesso restrito por área.**
- **Colaboradores e terceiros: Acesso limitado, conforme necessidade e contrato.**

4. Tecnologias: Firewall, criptografia, monitoramento de redes, backups seguros e autenticação de dois fatores (2FA).

5. Responsabilidades: Diretoria lidera, gestores aplicam, colaboradores cumprem, TI implementa e monitora.

6. Normas: Proibição de compartilhar senhas, bloqueio de dispositivos não autorizados, reporte de incidentes e atualizações regulares.

7. Sanções: Advertências, suspensão de acessos ou rescisão contratual, dependendo da gravidade.

8. Revisão: Atualização semestral ou em caso de mudanças significativas.

Monitoramento: Auditorias e relatórios periódicos para avaliar a eficácia

atenda ao processo escolhido no item 1 da etapa 2 apresentando ameaças/vulnerabilidades e proposta de solução.

Tabela 6- Suporte Técnico de Atendimento ao Cliente

Informação	Origem	Processamento/ Transformação	Saída	Ameaças/Vulnerabilidades	Proposta de Solução
O sistema de gerenciamento de pedidos ficou indisponível após uma atualização de software.	Cliente	Registro do problema no sistema de tickets com informações detalhadas pelo cliente.	Classificação do chamado.	Erro na classificação do tipo de chamado.	Implementação de um sistema de triagem inicial para ajudar a classificar com precisão.

Verificado que a falha ocorreu logo após a atualização do sistema. o do login.	Suporte Técnico-Nível 1	Análise do problema e diagnóstico técnico inicial.	O problema não foi solucionado com configurações básicas. Encaminhado para Nível 2	Diagnóstico incorreto, prolongado a resolução.	Treinamento técnico e checklists de diagnóstico detalhados para a equipe de suporte.
Detectado conflito entre a nova versão do software e o banco de dados.	Suporte Técnico-Nível 2	Análise detalhado	Correção na integração e reversão parcial da atualização.	Tentativa de solução inadequada em Nível 2.	Treinamento técnico e checklists de diagnóstico detalhados para a equipe de suporte.
Serviço foi restaurado?	Suporte Técnico-Nível 2	Confirmação de solução junto ao cliente.	Confirmação de resolução.	Insatisfação do cliente com a solução.	Implementação de uma política de retorno para ajustar soluções até a satisfação com cliente.
Serviço restaurado	Cliente	Coleta de Feedback após fechamento do chamado.	Feedback do cliente.	Feedback insuficiente ou inexistente.	Solicitação ativa de Feedback por meio de formulário simples.
O sistema está mais lento ou apresenta erros intermitentes?	Equipe de Qualidade	Análise de Feedback para identificar melhorias.	Plano de melhorias.	Falta de ações efetivas para resolver problemas recorrentes.	Processo de revisão periódica com base nos Feedbacks para aprimorar o atendimento.
Monitoramento estendido para garantir estabilidade.	Sistema de Monitoramento	Geração de relatórios de desempenho e indicadores.	Relatório de KPIs.	Falta de monitoramento contínuo ou dados incorretos.	Implementação de um sistema de monitoramento automático e auditorias de qualidade.
Sugestões para automatizar partes do processo de atendimento e suporte, como triagem de chamados.	Equipe de Atendimento e Suporte	Análise de processos e identificação de ajustes necessário.	Ações de melhoria implementada.	Falta de alinhamento entre equipe de atendimento e suporte.	Realização de reuniões regulares entre as equipes para avaliação dos processos e alinhamento das práticas.

2 Definir *Hardware* de servidor completo para atender ao modelo de sistema de informação construído no item 1, justificando cada escolha e mostrando o CAPEX e OPEX.

Hardware de Servidor para Sistema de Suporte Técnico e Atendimento ao Cliente da Compugraf

Tabela 7: Suporte Técnico e Atendiento ao Cliente

Serviços	Especificação	Justificativa	CAPEX (Investimento inicial)	OPEX (Custos operacionais)
EC2 (Elastic Compute Cloud)	2x t3.large (8 GB RAM)	Para suportar cargas mais altas e usuários simultâneos. Usar **Auto Scaling** para ajustar automaticamente a quantidade de instâncias de acordo com a demanda (mínimo 2, máximo 4 instâncias).	O modelo da AWS elimina investimentos iniciais (CAPEX), pois os custos são operacionais.	R$ 1.440,00
RDS (Relational Database Service)	db.t3.small (Multi-AZ)	Para lidar com maior volume de consultas. **Multi-AZ Deployment** (redundância em outra zona de disponibilidade) para alta disponibilidade.	-	R$ 177,60
EFS (Elastic File System)	100 GB (Bursting)	**Throughput Mode: Bursting** para gerenciar picos de acesso com melhor custo-benefício. Aumentar o armazenamento para **100 GB** para lidar com arquivos e logs mais volumosos.	-	R$ 180,00
S3 (Simple Storage Service)	200 GB Standard	Manter o armazenamento em **S3 Standard** para backups e logs,	-	R$ 27,60

ELB (Elastic Load Balancer)	Application Load Balancer	É mais eficiente para gerenciar múltiplas instâncias com tráfego de sistema web.	-	R$ 195,90
CloudWatch	Logs e alarmes	**logs detalhados e alarmes personalizados** para monitorar CPU, memória, e erros críticos.	-	R$ 90,00
Backup (RDS e EFS)	100 GB (RDS/EFS)	Maior capacidade de backup para cobrir o RDS e EFS.	-	R$ 60,00
Total mensal				R$ 2.170,86

Fonte: https://aws.amazon.com/pt/

3 Para este item a equipe terá de desenvolver um Script em C# que deverá ser entregue em um arquivo compactado com esse documento. Este script terá um menu com três opções de inventário do computador:

1. *Hardware*
2. *Software*
3. *Hardware e Software*

InventarioComputador.zip

4 Realizar uma análise de riscos/continuidade/contingência dos itens de segurança física e lógica encontrados no item 5 da etapa 2.

O quadro a seguir apresenta uma análise de riscos, continuidade e contingência relacionada a itens de segurança física e lógica. Cada ativo avaliado é associado às respetivas ameaças, vulnerabilidades, riscos, e medidas de continuidade e contingência recomendadas, com o objetivo de mitigar impactos e garantir a segurança das operações.

Tabela 8- Análise de Riscos, continuidade e contingências de Segurança Física e Lógica dos itens

Ativo	Ameaça	Vulnerabilidade	Riscos	Continuidade	Contingência
Servidores	Acesso físico não autorizado	Falta de controle de acesso adequado	**Probabilidade:** Média-Alta **Impacto:** Alto (interrupção de serviços).	Backups regulares dos dados armazenados; redundância de servidores; monitoramento contínuo.	Implementar failover automático; restaurar rapidamente serviços afetados; capacitar equipe para respostas imediatas.
Dados de clientes	Ataques cibernéticos	Falhas na gestão de acessos e autenticação	**Probabilidade:** Alta **Impacto**: Muito alto (vazamento de dados sensíveis e sanções legais).	Monitoramento de acessos; backups criptografados e armazenamento em local seguro; adoção de MFA.	Comunicação com autoridades e clientes; implementar políticas de mitigação imediata de danos causados pelo vazamento.
Dispositivos móveis	Roubo ou perda de dispositivos	Ausência de criptografia em dados móveis	Probabilidade: Média Impacto: Médio-Alto (exposição de dados sensíveis e interrupção de trabalho remoto).	Configuração de sistemas de gerenciamento de dispositivos móveis (MDM); backups automáticos; capacitação de usuários.	Apagar remotamente dispositivos perdidos ou roubados; bloquear acesso a sistemas corporativos comprometidos.

Tabela 9: Cont.

Banco de dados	Roubo ou perda de dados	Falha de criptografia e backup inadequado	Probabilidade: Média Impacto: Muito alto (perda de dados críticos e consequências legais severas)	Backups regulares em local seguro; adoção de criptografia para dados em trânsito e repouso; treinamento de equipes.	Restaurar dados por meio de backups seguros; ativar planos de resposta a incidentes para recuperação rápida.

Sistemas de software	Exploração de vulnerabilidades	Software desatualizado ou não corrigido	Probabilidade: Alta Impacto: Alto (comprometimento operacional e de dados).	Atualizações regulares (patch management); auditorias de segurança; monitoramento automatizado de vulnerabilidades.	Reverter para versões seguras; aplicar patches emergenciais; ativar planos de resposta para minimizar paralisações.
Equipamentos de rede (roteadores, interruptores)	Invasão e comprometimento	Configurações padrão não alteradas, firmware desatualizado	Probabilidade: Média-Alta Impacto: Alto (comprometimento da infraestrutura e de dados trafegados).	Segmentação da rede; backups de configurações; atualização regular de firmware e protocolos de segurança.	Reconstrução rápida de configurações; isolamento de segmentos comprometidos; mobilização de equipe de suporte técnico.