Universidade Pontifícia Católica de Minas Gerais (PUC Minas)

Curso: Segurança da Informação

Disciplina: Projeto: Fundamentos de Sistemas

Proposta de Soluções Seguras

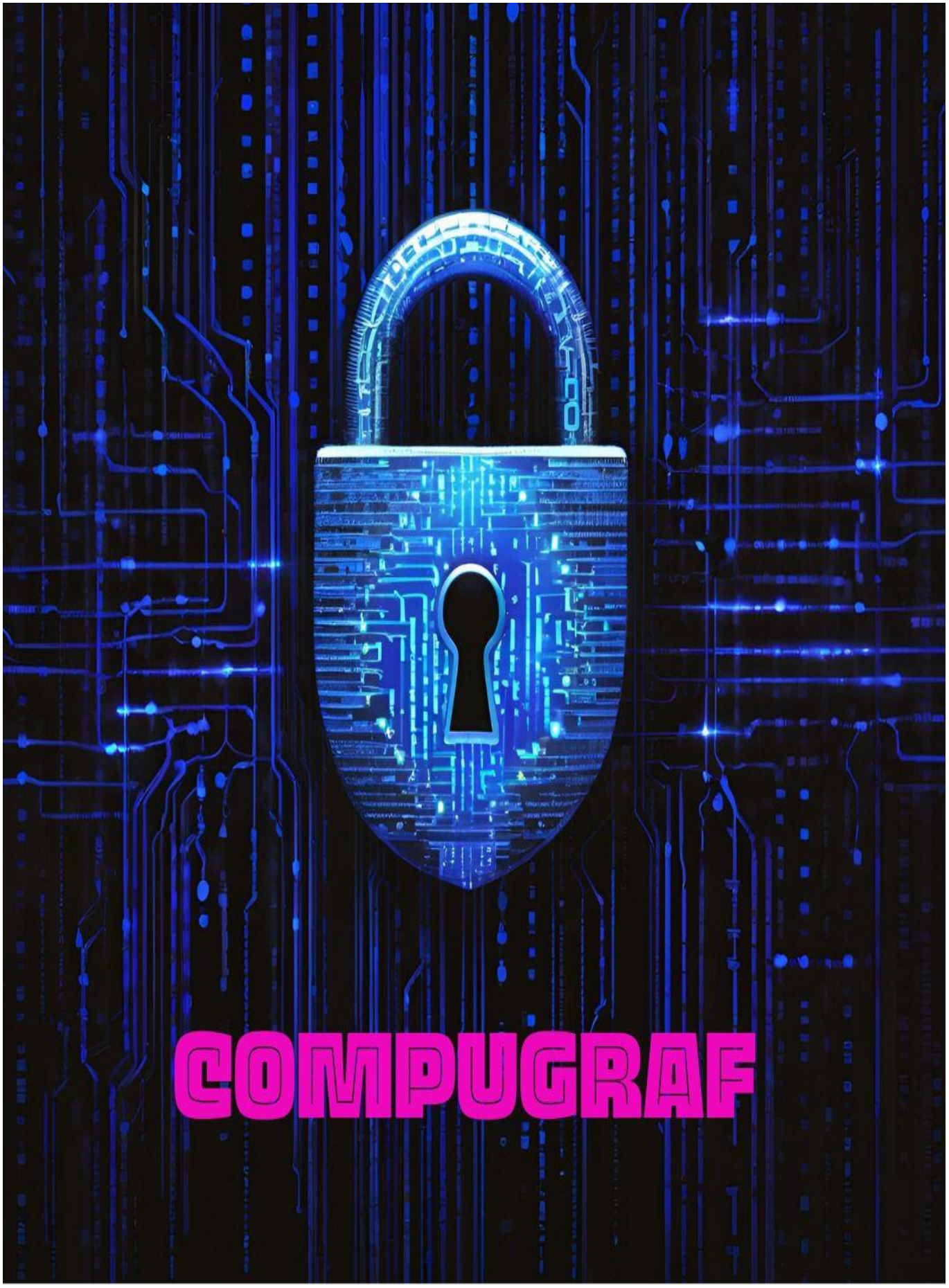
Equipe de Trabalho
Alexandre Zacura Luiz 877868

Marcio de Souza Braga 875364

Pedro Manoel 877798

Yasmin da Silva Martins Siqueira 874756

Orientador
Pedro Ivo Alexandre de Oliveira


COMPUGRAF

SUMÁRIO

1. Introdução

A empresa Compugraf é uma organização importante no setor de tecnologia da informação, com uma longa trajetória de sucesso e inovação. Este trabalho tem como objetivo apresentar uma análise detalhada da empresa, justificando a relevância de entender sua atuação no mercado.

1.1. Justificativa

A segurança da informação é um tópico fundamental para as empresas na era digital, especialmente diante das crescentes ameaças cibernéticas. Neste contexto, a Compugraf destaca-se como uma referência de excelência no desenvolvimento de soluções de segurança adaptáveis. Este estudo busca oferecer propostas concretas e eficazes para empresas, baseadas nas melhores práticas observadas na Compugraf, alinhadas com as regulamentações de proteção de dados, como a LGPD.

1.2. Apresentação da Empresa Compugraf

A Compugraf é uma empresa renomada no setor de tecnologia da informação, destacando-se pela oferta de soluções inovadoras em hardware e software, bem como pela prestação de serviços de consultoria e suporte técnico. Fundada em 1990, a empresa conquistou uma sólida reputação no mercado, atendendo a uma ampla gama de clientes. Seu compromisso com a

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.

2.1 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.

1 Leis relacionadas a TI que impactam o negócio

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

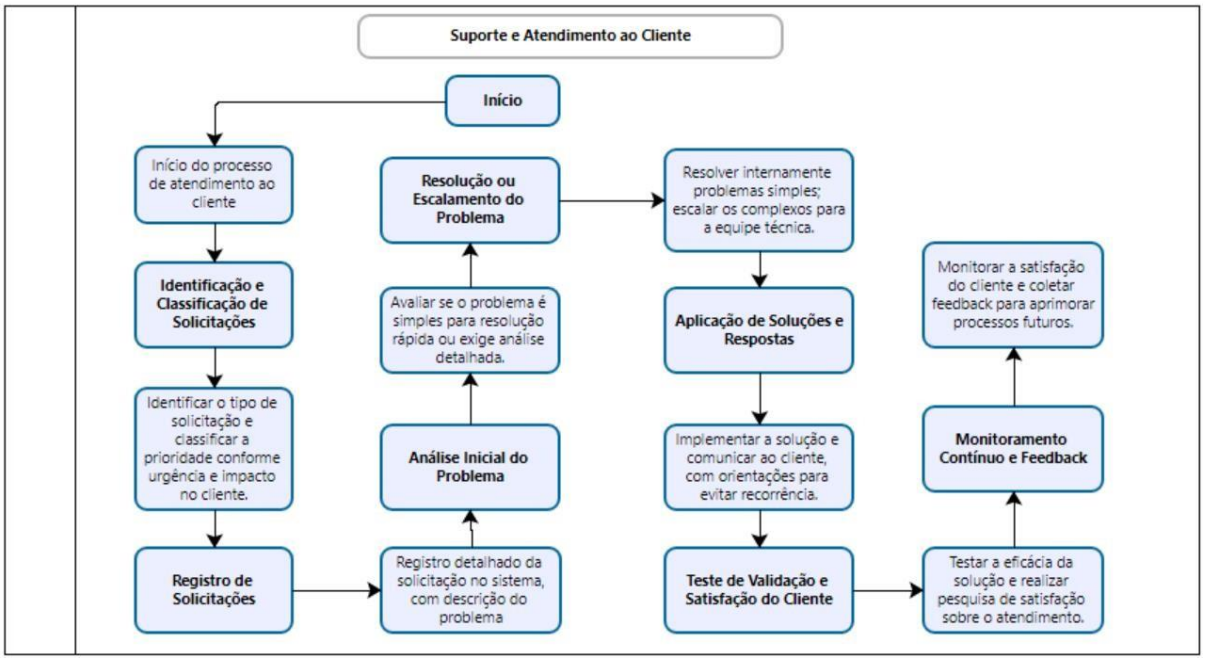
	regras rigorosas sobre coleta, armazenamento e tratamento de dados pessoais, garantindo a privacidade e segurança dos usuários, em linha com a LGPD. **Retenção de Registros de Conexão :** Se a Compugraf armazenar registros de conexão e navegação, deve mantê-los sob sigilo por, no máximo, 12 meses e só 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.
RGPD	**Consentimento e Bases Legais :** A Compugraf deve garantir que o tratamento de dados pessoais seja baseado em uma das bases legais previstas pelo RGPD, como consentimento, execução de contratos ou legítimo interesse. **Direitos dos Titulares :** A empresa deve assegurar que os direitos dos titulares sejam respeitados, incluindo acesso, retificação, exclusão, portabilidade e oposição ao tratamento de dados. **Segurança de Dados :** A Compugraf deve implementar medidas técnicas e organizacionais adequadas para garantir a segurança dos dados pessoais, prevenindo acessos não autorizados e vazamentos. **Notificação de Violações :** Em caso de violação de dados, a empresa deve notificar a autoridade supervisora competente e os titulares afetados dentro de 72 horas após a descoberta do incidente.

Matriz de relacionamento de processos organizacionais e leis.

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.

Processo	Leis a serem observadas
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.



2. **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.**

3.Mapear itens relacionados à 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	Joao Silva	Equipe de TI	Acesso não monitorado a credenciais	Software com senhas à todas as credenciais. Perigo de movimentação lateral

4.Identificar dispositivos pessoais utilizados na organização.

Setor	Dispositivo	Proprietário	Usuários	Risco	obs
Marketing	Smartphone pessoal	Carlos Oliveira	Carlos Oliveira	Comunicaçãoexterna 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.

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

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

6. 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 da Compugraf

---

1. Introdução

A **Compugraf**, com mais de 40 anos de experiência no mercado brasileiro, é líder em soluções de cibersegurança e proteção de dados. Como parte do compromisso contínuo com a integridade e segurança da informação, a empresa desenvolveu esta **Política de Segurança da Informação (PSI)**. O objetivo é fornecer diretrizes claras e eficazes para proteger os ativos de informação, reduzir riscos cibernéticos e assegurar a conformidade com as leis e regulamentações aplicáveis, como a **Lei Geral de Proteção de Dados (LGPD)**.

Esta política abrange todas as áreas de operação da Compugraf, incluindo colaboradores, prestadores de serviço, parceiros, fornecedores e qualquer parte que tenha acesso aos ativos de informação da empresa.

---

2. Princípios de Segurança

A Compugraf adota princípios fundamentais de segurança da informação para garantir a proteção adequada de todos os ativos. Estes princípios são:

- **Confidencialidade**: Garantir que informações sensíveis e críticas estejam acessíveis apenas para pessoas autorizadas.
- **Integridade**: Assegurar que as informações sejam exatas e completas, evitando alterações não autorizadas.

- **Disponibilidade**: Garantir que as informações e sistemas estejam disponíveis para acesso legítimo quando necessário.
- **Autenticidade**: Verificar a identidade de todos os usuários e sistemas antes de permitir o acesso.
- **Responsabilidade**: Definir claramente as responsabilidades de cada colaborador, garantindo que cada um entenda e cumpra suas obrigações de segurança.

---

3. Gerenciamento de Acesso

O gerenciamento de acesso é um aspecto crítico da segurança da informação. Na Compugraf, adotamos práticas rigorosas para garantir que o acesso aos sistemas e dados seja controlado e limitado com base nas funções e responsabilidades de cada colaborador.

Controle de Acesso: Todos os acessos a sistemas de informação são baseados no princípio do **menor privilégio**, garantindo que os usuários tenham acesso apenas às informações necessárias para o desempenho de suas funções.

Autenticação e Autorização: São utilizadas autenticações robustas, como senhas fortes e autenticação multifator (MFA), para garantir a identidade dos usuários.

Revisão de Acessos: Os acessos são revisados periodicamente, garantindo que privilégios desnecessários sejam removidos, minimizando o risco de acessos indevidos

Desativação de Contas: O acesso de colaboradores que deixam a empresa ou mudam de função é imediatamente desativado ou ajustado conforme necessário.

---

4. Segurança Física e Ambiental

A Compugraf implementa medidas de segurança física e ambiental para proteger as instalações e ativosde informação contra ameaças físicas, como acesso não autorizado, desastres naturais, roubo e sabotagem.

- **Controle de Acesso Físico**: Todas as áreas sensíveis, como datacenters, são protegidas por sistemas de controle de acesso com cartões, biometria ou senhas. Apenas pessoas autorizadaspodem entrar nessas áreas.
- **Monitoramento de Ambientes**: Sistemas de câmeras de segurança (CFTV) são utilizados paramonitorar áreas críticas. O monitoramento é contínuo e registrado.
- **Proteção Ambiental**: Sistemas de climatização, proteção contra incêndios e desastres naturaissão implantados para proteger os ativos físicos da empresa.
- **Proteção contra Desastres**: Planos de contingência e recuperação de desastres estão em vigorpara garantir a continuidade dos negócios em caso de eventos catastróficos.

---

5. Segurança de Redes e Comunicações

A segurança das redes de comunicação da Compugraf é fundamental para proteger os dados em trânsito e garantir que as informações trocadas entre colaboradores, clientes e parceiros sejam segurase confiáveis.

- **Segurança de Redes**: Implementamos Firewall, sistemas de detecção e prevenção de intrusões(IDS/IPS) e segmentação de redes para proteger contra acessos não autorizados e ataques externos.
- **Criptografia**: Todas as comunicações sensíveis, internas e externas, são protegidas por meio decriptografia de ponta a ponta (ex.: TLS, VPN). Dados em repouso também são criptografados conforme necessário.
- **Monitoramento de Rede**: O tráfego de rede é monitorado continuamente para detectar eresponder a atividades suspeitas ou tentativas de invasão.
- **Proteção de E-mails**: Sistemas de filtragem e criptografia de e-mails são implementados paraproteger contra ameaças como phishing e malware.

---

6. Gestão de Incidentes de Segurança

A Compugraf adota uma abordagem proativa para a **gestão de**

incidentes de segurança. A empresa implementa um processo estruturado para detectar, responder e corrigir incidentes de segurança deforma rápida e eficaz.

- **Detecção e Registro de Incidentes**: Qualquer evento de segurança que comprometa a confidencialidade, integridade ou disponibilidade da informação deve ser imediatamente identificado e registrado.
- **Resposta a Incidentes**: Uma equipe dedicada é responsável pela investigação, mitigação econtenção dos incidentes, minimizando seu impacto nos negócios.
- **Comunicação de Incidentes**: Incidentes de segurança relevantes são comunicados às partesinteressadas, incluindo autoridades regulatórias (ANPD) e clientes, quando aplicável.
- **Análise Pós-Incidente**: Após cada incidente, uma análise detalhada é realizada para identificara causa raiz e implementar melhorias no processo de segurança, prevenindo ocorrências futuras.

---

7. Conscientização e Treinamento em Segurança

A conscientização dos colaboradores é fundamental para garantir a eficácia das políticas de segurança. Na Compugraf, oferecemos programas contínuos de **treinamento em segurança da informação** para todos os colaboradores e parceiros.

- **Programas de Conscientização**: Treinamentos periódicos são realizados para garantir que todosos colaboradores estejam cientes das melhores práticas de segurança, riscos cibernéticos e suas responsabilidades.
- **Simulações de Ataques**: Realizamos exercícios como simulações de phishing para educar emedir a resposta dos colaboradores a ameaças comuns.
- **Política de Aceitação**: Todos os colaboradores são obrigados a ler e aceitar formalmente aPolítica de Segurança da Informação e seus anexos.

---

8. Avaliação e Melhoria Contínua

A **avaliação e melhoria contínua** é essencial para garantir que a política de segurança da Compugrafacompanhe a evolução das ameaças cibernéticas e o desenvolvimento tecnológico.

- **Auditorias Internas e Externas**: Auditorias periódicas são conduzidas para verificar aconformidade com a política e identificar áreas que necessitam de melhoria.
- **Gestão de Vulnerabilidades**: São realizados testes regulares de vulnerabilidade e avaliações derisco para garantir que novas ameaças sejam detectadas e corrigidas.
- **Revisão da Política**: Esta política é revisada regularmente, garantindo que esteja sempreatualizada em relação às novas regulamentações, tecnologias e ameaças.

9. Conformidade Legal e Regulatória

A Compugraf está comprometida em garantir a conformidade com todas as legislações e regulamentações de proteção de dados e segurança das informações aplicáveis.

- **Lei Geral de Proteção de Dados (LGPD)**: Todos os tratamentos de dados pessoais realizados pela Compugraf estão em conformidade com a LGPD, garantindo que os direitos dos titularessejam respeitados e que o uso de dados seja transparente e adequado.
- **Normas Internacionais (ISO/IEC 27001)**: A Compugraf adota as melhores práticas e normas internacionais de segurança da informação, como a **ISO/IEC 27001**, para manter um Sistema de Gestão de Segurança da Informação (SGSI) robusto e eficaz.
- **Regulamentações Setoriais**: Asseguramos a conformidade com regulamentações específicas desetores onde atuamos, como o financeiro, saúde e administração pública.

10. Responsabilidades

As responsabilidades pela segurança da informação são claramente definidas e distribuídas entre osdiferentes níveis da organização.

- **Diretoria Executiva**: Responsável por fornecer suporte estratégico e garantir que a segurançada informação seja uma prioridade em todas as operações da empresa.
- **Gerência de Segurança da Informação**: Responsável pela implementação, gestão e revisão daspolíticas e controles de segurança.
- **Colaboradores**: Cada colaborador é responsável por seguir as

diretrizes estabelecidas nestapolítica e reportar imediatamente quaisquer incidentes ou comportamentos suspeitos.

- **Fornecedores e Parceiros**: Devem aderir às mesmas normas de segurança e privacidade definidas pela Compugraf, sob pena de penalizações contratuais em caso de não conformidade.

11. Disposições Finais

Esta política está disponível para todos os colaboradores e interessados e deve ser adotada como base para todas as operações e decisões relacionadas à segurança da informação naCompugraf.

Compugraf – Há 40 anos garantindo a segurança digital com inovação, experiência ecompromisso.

Etapa 3 – Projeto Fundamentos de Sistemas.

1. **Construir um modelo de sistema de informação (no formato de um quadro) que atenda ao processo escolhido no item 1 da etapa 2 apresentando ameaças/vulnerabilidades e proposta de solução.**

Suporte Técnico de Atendimento ao Cliente da Compugraf

Informação	**Origem**	**Processamento/ Transformação**	**Saída**	**Ameaças/Vulnerabilidades**	**Proposta de Solução**
Chamado do Cliente	Cliente	Registro do chamado e classificação (Atendimento/Suporte).	Classificação do chamado.	Erro na classificação do tipo de chamado.	Implementação de um sistema de triagem inicial para ajudar a classificar com precisão
Diagnóstico Técnico	Suporte Técnico	Análise do problema e diagnóstico técnico inicial.	Diagnóstico preliminar.	Diagnóstico incorreto, prolongado a resolução.	Treinamento técnico e checklists de diagnóstico detalhados para a equipe de suporte.
Solução de Problemas Nível 1	Suporte Técnico	Aplicações de soluções básicas(Nível 1).	Resolução de problemas simples.	Tentativa de solução inadequada em Nível 1.	Diretrizes para escalonamento rápido ao Nível 2, se necessário.
Solução de Problemas Nível 2	Especialistas Técnicos (Nível2)	Aplicações de soluções avançadas (Nível 2).	Resolução de problemas complexo.	Falta documentação clara para soluções complexas.	Criação de uma base de dados para registrar soluções de problemas comuns e complexos.
Verificação com o Cliente	Suporte Técnico e Cliente	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.

Coleta de Feedback	Cliente	Coleta de Feedback após fechamento do chamado.	Feedback do cliente.	Feedback insuficiente ou inexistente.	Solicitação ativa de Feedback por meio de formulário simples.
Análise de Feedback	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 e Relatórios	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.
Reunião de Revisão de Processos	Equipamento 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

Componente	Especificação	Justificativa	CAPEX (Investimento inicial)	OPEX (Custos operacionais)
Servidor Principal	Dell PowerEdge R750 ou HPE ProLiant DL380	Servidor com maior escalabilidade e suporte para workloads de AI/ML. Permite upgrades futuros e melhor virtualização.	R$87.150,00 a R$104.580,00	R$17.400,00 (Manutenção Anual)
Processador	2 x Intel Xeon Gold 5317 3.0 GHz, 16-Core	Maior cache e threads para melhorar eficiência em múltiplas VMs.	R$ 11.554,20	

Memória RAM	256 GB DDR4	Expansão de memória para suportar picos de carga e mais requisições simultâneas.	R$ 11.359,74	
Armazenamento	8 TB SSD NVMe em RAID 10 (dados críticos) + 12 TB HDD (logs e backups)	A combinação oferece **um equilíbrio entre performance e custo**, com **alta disponibilidade e segurança** para dados importantes e uma estratégia de armazenamento eficiente.	R$ 6.761,93	
Sistema de Backup	Synology NAS 24 TB em RAID 6 + Veeam Backup + Backup em Nuvem (AWS S3 ou Azure)	Backup em múltiplas camadas (local e nuvem), alta disponibilidade, fácil recuperação, e maior proteção contra perda de dados.	R$ 29.000,00	
Fonte de Alimentação Redundante	2 x 1100 W Redundant Power Supplies	Fontes redundantes de maior capacidade, suportam upgrades de hardware.	R$ 6.960,00	
Sistema de Rede	2 x Cisco Catalyst 9300 Switch (10GbE) + Firewall (Fortinet FortiGate)	Switches de alta durabilidade e segurança com conectividade 10GbE para escalabilidade de rede.	R$ 43.500,00	R$ 11,600,00 (Manutenção e Licenças)
Unidade de Backup de Energia (UPS)	APC Smart-UPS 5000VA	UPS de maior capacidade oferece suporte de energia prolongado para demandas críticas.	R$ 20.300,00	R$ 2.900,500(Troca de Bateria a cada 2-3 anos)
Software de Virtualização e Sistema Operacional	VMware vSphere Enterprise + Windows Server 2022	VMware vSphere Enterprise permite automação e monitoramento avançado de VMs.	R$ 29.000,00	R$ 4.060,00 (Suporte Anual de Licenças)
Sistema de Monitoramento	Prometheus + Grafana	Prometheus e Grafana para monitoramento avançado e análise em tempo real de toda a infraestrutura.	R$ 10.440,00	R$3.480,00 (Suporte)

SLA e Contrato de Suporte Técnico	Dell ProSupport Plus - Resposta em 4 horas	Suporte técnico rápido com SLA de 4 horas para garantir continuidade do atendimento.	R$ 14.500,00	R$8.700,00 (Renovação Anual)

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.

ATIVO	AMEAÇA	VULNERABILIDADE	RISCOS	CONTINUIDADE	CONTIGÊNCIA
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.

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.