### Galeria

### **Trabalho referente ao projeto do 1º ciclo 2/2024**

Turma 02 Grupo 02

PSI

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CONECTATEL

Belo Horizonte Novembro de 2024

### **Política de Segurança da Informação**

PSI-001-2024

Versão 1.0

Classificação: Interna

Última revisão: 03/11/2024

1. Introdução ............................................................................................................................... 6

1.1. Objetivo ............................................................................................................................ 6

1.2. Escopo .............................................................................................................................. 7

1. Princípios de Segurança .......................................................................................................... 7  
   2.1. Segurança da informação................................................................................................. 7

2.2. Confidencialidade ............................................................................................................ 7

2.3. Integridade ...................................................................................................................... 8

2.4. Disponibilidade ................................................................................................................ 8

1. Glossário ................................................................................................................................. X
2. Gerenciamento de Acesso ...................................................................................................... X

3.1. Gerenciamento de Acesso ............................................................................................... X

3.2. Autenticação .................................................................................................................... X

3.3. Autorização ...................................................................................................................... X

1. Segurança Física e Ambiental ................................................................................................. X

5.1. Proteção de Instalações ...................................................................................................X

5.2. Controle de Acesso Físico ................................................................................................ X

5.3. Segurança Ambiental ....................................................................................................... X

1. Segurança de Redes e Comunicações ..................................................................................... X

6.1. Proteção de Redes ........................................................................................................... X

6.2. Monitoramento e detecção de intrusões ........................................................................ X

1. Gestão de Incidentes de Segurança ........................................................................................ X

7.1. Resposta a Incidentes ...................................................................................................... X

7.2. Relatórios de Incidentes .................................................................................................. X

1. Conscientização e Treinamento em Segurança ...................................................................... X

8.1. Programa de Conscientização .......................................................................................... X

8.2. Treinamento em Segurança ............................................................................................. X

1. Avaliação e Melhoria Contínua ............................................................................................... X

9.1. Auditorias de Segurança .................................................................................................. X

9.2. Revisão de Políticas e Procedimentos ............................................................................. X

9.3. Análise de Riscos ............................................................................................................. X

9.4. Medição de Desempenho ............................................................................................... X

1. Conformidade Legal e Regulatória ......................................................................................... X

10.1. Conformidade com Leis e Regulamentações ................................................................ X

10.2. Gerenciamento de Vulnerabilidades e Patches ............................................................ X

1. Responsabilidades ................................................................................................................. X

11.1. Direção .......................................................................................................................... X

11.2. Equipe de Segurança da Informação ............................................................................ X

11.3. Funcionários ................................................................................................................. X

### **1.0. Introdução**

### **1.1. Objetivo da Política de Segurança da Informação**

### Estabelecer diretrizes que permitam aos colaboradores, associados, clientes e prestadores de serviços da ConectaTel seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa, das informações e do indivíduo. Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da ConectaTel quanto à:

● Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

● Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

● Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário, com as devidas autorizações.

### **1.2. Escopo da Política de Segurança da Informação**

Esta Política se aplica a todos os ativos de informação da ConectaTel, incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam ou processam as informações da Conectatel. Esta política se aplica em todas as instalações físicas administradas ou utilizadas pela ConectaTel e entidades subsidiárias. Estrategicamente, esta política se aplica a todos executivos, diretores e acionistas da ConectaTel, isso é, aqueles responsáveis pelos planos de longo prazo da empresa com acesso a informações confidenciais financeiras, administrativas e operacionais. Taticamente, esta política se aplica a todos os gestores, gerentes e supervisores da ConectaTel responsáveis pelo gerenciamento e supervisão dos atendentes em nível operacional, dado que os mesmos possuem acesso direto a ativos confidenciais de clientes e funcionários da ConectaTel. Em nível operacional, esta política afeta a todos os funcionários de responsáveis pelo atendimento direto ao cliente, sejam eles atendentes de telemarketing, vendedores, estagiários ou jovens aprendizes, dado que na execução diária do exercício da profissão estes funcionários lidam com informações sensíveis e confidenciais de clientes, sejam essas informações novas sendo adicionadas ao sistema ou informações já salvas. Além disso, cabe notar que esta política não é válida para nenhum dos clientes que fazem uso dos serviços oferecidos pela ConectaTel, dado que os mesmos não têm acesso por definição aos ativos de segurança que a ConectaTel possui. É também necessário destacar que é obrigação de cada colaborador manter-se atualizado em relação à PSI e aos procedimentos e normas relacionadas, buscando ajuda do Departamento de Tecnologia da Informação caso não esteja totalmente seguro quanto à aquisição, uso ou descarte das informações.

**2.0. Princípios de segurança**

### **1.1. Segurança da informação**

Definida como a proteção da informação de vários tipos de ameaça para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades do negócio.  
  
  
**1.2. Confidencialidade**

O princípio da confidencialidade determina que certa informação, fonte ou sistema deve estar acessível apenas a pessoas autorizadas. Caso um indivíduo não autorizado acesse, intencionalmente ou não, uma informação sigilosa, haverá quebra de confidencialidade.

**1.3. Integridade**  
  
  
 O princípio da integridade estabelece que certa informação deve ser correta, confiável e sem alterações não autorizadas. Ou seja, os dados devem permanecer intocados, por meio de precauções para que eles não sejam modificados ou eliminados sem autorização, para preservar sua confiabilidade e originalidade. Se isso não ocorrer, as informações podem ser interpretadas erroneamente, gerando rupturas no compliance do negócio e, em algumas situações, sanções relevantes.  
  
  
**1.4. Disponibilidade**  
  
  
 O princípio da disponibilidade determina que a informação deve estar sempre acessível para uso legitimo de pessoas autorizadas. Para garantir essa disponibilidade, e imperativo implementar uma seria de controles e práticas robustas que abordem tanto a prevenção quanto a mitigação de riscos.

**3.0. Glossario**  
  
  
**Colaborador:** Empregado, estagiário ou menor aprendiz da instituição.   
  
**Dados:** Conjunto de fatos, valores ou ocorrências em estado bruto, que, quando processado ou agrupado, produzem informações.  
  
  
**4.0. Gerenciamento de Acesso**

**4.1. Controle de Acesso**

O acesso às informações de login dos usuários é estritamente restrito apenas aos atendentes em nível operacional que necessitam utiliza-las para autenticar o usuário e ao nível estratégico com acesso ao banco de dados da empresa que precisem desses dados para funções de marketing e prestação de contas. Qualquer reinvindicação aos dados de login de clientes vindo de outro setor deve recorrer ao setor de TI para sanar o problema.

**4.2. Autenticação**

A autenticação do cliente ao sistema é dada com o uso de três informações, sendo elas o nome completo, CPF e endereço de e-mail, onde em caso de conflito no sistema ou erro, ou operador pode escolher pedir mais informações, sendo essas endereço e número de telefone. Qualquer informação além das citadas nessa seção que seja pedida pelo operador configura como imprópria e além da autorização do mesmo, podendo levar a punição. O controle de acesso dessas informações é descrito na seção anterior. É responsabilidade do operador a autenticação do cliente e, portanto, confirmação de sua identidade.

**4.3. Autorização**

Tem autorização ao acesso de dados de login dos clientes atendentes em níveis operacionais, colaboradores em nível tático como gerentes e supervisores, e colaboradores em nível estratégico, como executivos. A modificação dessas informações de forma a entrar de acordo com as necessidades do cliente deve ser feita pelo operador ou supervisor, caso seja necessário este último. A permissão de modificação em larga escala das informações dos clientes ou modificação de sistema é reservada somente a colaboradores de nível estratégico, sendo estritamente proibido a modificação de informações por livre arbítrio dos operadores, estando sujeito a punição.

**5.0.** **Segurança Física e Ambiental**

**5.1. Proteção de Instalações**

Para a integridade das informações contidas em servidores, discos rígidos e quaisquer formas de memória, é necessário que haja um sistema de condicionamento de ar que mantenha a sala em temperatura ambiente, evitando quedas e altas bruscas de temperatura, que podem danificar os aparelhos. Além disso, para assegurar a integridade das informações, é essencial uma fonte de energia ininterrupta que alimente os dispositivos de TI.

**5.2. Controle de Acesso Físico**

Para garantir a confidencialidade das informações e disponibilidade das mesmas somente a pessoas autorizadas, é necessário estabelecer uma série de medidas de controle de acesso físico. É necessário assegurar a entrada de somente pessoas autorizadas ao prédio da empresa, portanto havendo um sistema de portaria para autenticação de funcionários e registro. A portaria registra os funcionários e os entrega cartões de acesso para que não seja necessário futuro uso da portaria pelos mesmos para entrar na empresa. Já dentro da empresa, é necessário garantir iluminação adequada para o uso correto de câmeras de vigilância por meio de um monitoramento constante. Os cartões de acesso devem ser manufaturados por meio de uma divisão de acesso em camadas, garantido a entrada somente de pessoas autorizadas em certas salas, como a sala de servidores. Os sistemas de restrição de acesso devem possuir logs de entrada e saída com as informações daqueles que entraram e saíram baseando-se no cartão de acesso.

**5.3. Segurança Ambiental**

Para garantir a integridade e disponibilidade da informação, é necessário uma série de medidas para lidar com desastres naturais e ambientais que podem impactar diretamente os ativos. É necessário instalar sistemas de detecção precoce e supressão de incêndio, como sistemas de gás inerte (para proteger os equipamentos eletrônicos sem danificá-los), fontes de alimentação redundantes, ou seja, múltiplas fontes de energia como geradores e UPS para garantir o fluxo constante de energia para os equipamentos de TI mesmo durante quedas de energia, conexões de rede redundantes para garantir a conexão constante à internet e as instalações devem ser projetadas para resistir a desastres naturais como inundações, terremotos e tempestades, sendo necessária resistência estrutural.

6.0. Segurança de Redes e Comunicações

6.1. Proteção de Redes

Para proteger as redes da comunicação contra ataques internos ou externos, evitando vazamento, corrupção de dados, e outros problemas, é necessário o uso de uma série de ferramentas em sinergia com monitoramento contínuo dos analistas. Para começar, é necessário a aplicação de um firewall para filtrar o tráfego de rede; aplicação de sistemas de detecção e prevenção de intrusões (IDS/IPS) para monitoramento contínuo da rede e impedimento de atividades suspeitas, controle de acesso para permitir que somente funcionários autorizados acessem recursos específicos, criptografia de dados para garantir a proteção dos dados em tráfego e em repouso mesmo em caso de interceptação, segmentação de redes para limitar a propagação de um ataque em caso de comprometimento, programas antimalware para impedir a execução de softwares maliciosos e proibição do uso de dispositivos externos sem análise prévia do departamento de TI, como pen-drives. Além disso, é necessário monitoramento contínuo dos analistas de rede para análise de tráfego e dos logs salvos pelas ferramentas utilizadas, como o firewall.

6.2. Monitoramento e Detecção de Intrusões

No processo de monitoramento e detecção, o trabalho dos analistas de rede se torna indispensável junto com o uso de softwares criados para tal. O uso de firewalls e sistemas de detecção e prevenção de intrusões (IDS/IPS) é imprescindível para esse processo, além de softwares antimalware. É necessário que estes softwares utilizados tenham função de logs e que esses logs sejam analisados periodicamente pelos analistas de rede de forma a evitar atividades suspeitas não detectadas pelo software.

7.0. Gestão de Incidentes de Segurança

7.1. Resposta a Incidentes

A resposta a incidentes de segurança deve seguir uma sequência lógica de etapas que garantam o tratamento correto de cada situação. Em primeiro lugar, a política de definição de incidentes deve ser clara para que todos os colaboradores possam identificar rapidamente quando uma questão é, de fato, um incidente de segurança. Um incidente de segurança é uma exploração de uma vulnerabilidade que leva a uma ameaça e pode incluir: acesso não autorizado, malware, phishing, vazamento de dados, falhas de configuração e denúncias internas ou externas. Em segundo lugar vem a identificação e registro do incidente. É necessário classificá-lo conforme sua natureza (malware, phishing, acesso não autorizado, etc), criar um registro de chamado específico no sistema de gerenciamente de incidentes (ITSM) detalhando a descrição do incidente e as informações relevantes fornecidas pelo usuário ou monitoramento. Caso o incidente seja crítico ou de alto risto, como vazamento de dados ou ransomware, é necessário notificação imediata a equipe de resposta a incidentes. Em terceiro lugar se dá a contenção e isolamento dos incidentes. Se o incidente envolver uma ameaça ativa (como malware ou ransomware), o analista ou responsável pela segurança da informação deve tomar medidas imediatas para isolar o sistema afetado, como desconectar o dispositivo comprometido da rede, bloquear a conta do usuário comprometida ou alterar senhas para prevenir acessos não autorizados. Caso o incidente seja classificado como complexo ou fora da capacidade do analista de segurança (como no caso de ataque DDoS ou exploração de vulnerabilidade crítica), o chamado deve ser escalado para a equipe de resposta a incidentes. No caso de escalonamento, a equipe de resposta a incidentes deve, em primeiro lugar, realizar a análise forense para entender a origem do ataque e a extensão do comprometimento. Dado isso, deve-se realizar a erradicação da ameaça (por exemplo, remoção de malware, aplicação de patches de segurança, correção de falhas de configuração de softwares) e então realizar a validação dos sistemas para garantir que os mesmos estão livres de qualquer vestígio de ataque ou comprometimento. Em quarto lugar, em caso de comprometimento de dados ou softwares, é necessário um processo de recuperação dos sistemas afetados utilizando backups. Assim que restaurados, deve-se monitorar estes sistemas para detectar qualquer sinal de reincidência do incidente. Em quinto lugar, a comunicação entre os analistas e a equipe de resposta a incidentes deve ser constante durante todo o processo de comprometimento. Em caso de necessidade de comunicação externa, caso ocorra vazamento de informações, é responsabilidade do departamento de comunicação, marketing ou relações públicas tratar da mesma. Por último, é necessário o encerramento do chamado e criação de um relatório pós-incidente que documente todas as ações realizadas e correções implementadas.

7.2. Relatórios de Incidentes

É necessário a comunicação constante entre os funcionários da empresa e a equipe de segurança da informação no que diz respeito a incidentes de segurança. Caso seja confirmado o reconhecimento de um funcionário sobre um incidente de segurança e sua falta de comunicação com o departamento de TI, ações administrativas podem ser tomadas. É função da equipe de segurança da informação a elaboração de relatórios completos sobre os incidentes de segurança, sendo necessário dos funcionários alheios somente sua comunicação quanto aos mesmos.

8.0. Conscientização e Treinamento em Segurança

8.1. Programa de Conscientização

É obrigatório um programa de conscientização que defina claramente conceitos básicos de segurança da informação e a função de cada colaborador na manutenção da mesma. Este programa deve ser composto por 8 partes, sendo as seguintes: “Introdução à Segurança da Informação”, onde será discutido o que é a segurança da informação, princípios básicos da mesma, exemplos de incidentes de segurança e apresentação de ameaças e riscos cibernéticos mais comuns; “Responsabilidades Individuais dos Funcionários”, onde será definido as responsabilidades de cada funcionário em relação à segurança da informação, com especificação de cargo, caso necessário. Além disso, deve ser ensinado os funcionários sobre a criação de senhas fortes, o que fazer ao identificar um possível incidente de segurança e a política de uso aceitável de dispositivos pessoais no trabalho; “Segurança no Uso de E-mails e Redes Sociais”, no caso dos funcionários que trabalham frequentemente com e-mails e redes sociais da empresa, é necessário saber reconhecer e-mails de phishing, o cuidado ao abrir anexos e links desconhecidos e a proteção dos dados pessoais deles mesmos e das empresas; “Segurança de Dispositivos e Dados Pessoais”, o objetivo dessa seção é orientar os funcionários que possuam informações sensíveis da empresa em seus aparelhos pessoais, especialmente funcionários do setor estratégico da empresa, como proteger seus dispositivos e informações pessoais. Deve ser apresentado uma política de segurança para dispositivos móveis e computadores pessoais, como criptografar dados e utilizar VPN, a importância do backup de dados e armazenamento seguro e a necessidade de evitar o uso de Wi-Fi públicas inseguras; “Políticas e Procedimentos de Segurança da Empresa”, o objetivo dessa seção é apresentar as políticas internas da segurança da informação, isso é, resumir ou mostrar por completo a PSI da empresa, juntamente com as ações que devem ser tomadas em caso de incidente; “Simulação de Ataques Cibernéticos”, durante o programa de conscientização, é necessário simular pelo menos um ataque cibernético, sendo necessário escolher um dos ataques cibernéticos mais comuns, como phishing ou engenharia social; “Avaliação e Feedback”, o objetivo dessa seção é avaliar a compreensão dos funcionários sobre o que foi aprendido no programa e pedir pelo feedback dos mesmos para futuras melhorias. Por último, é necessário que esse programa seja atualizado anualmente em busca de informações datadas ou novas que possam ser adicionadas.

8.2. Treinamento em Segurança

O treinamento exposto no programa de conscientização deve ser aplicado para todos os novos funcionários e antigos que não tenham o feito no ano. O programa deve ser aplicado anualmente para todos os funcionários da empresa, sem exceção. Simulações devem ser feitas regularmente pelo menos a cada trimestre com o objetivo de educar os funcionários em possíveis ameaças. É recomendável que as ameaças escolhidas sejam as mais frequentemente utilizadas por atacantes.