



|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

## TELEPUC – TELEMARKETING 2024

### POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

#### Sumário

|   |           |
|---|-----------|
| <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.....</b>       | <b>1</b>  |
| <b>1. INTRODUÇÃO.....</b>                             | <b>2</b>  |
| <b>2. OBJETIVOS .....</b>                             | <b>2</b>  |
| <b>3. ABRANGÊNCIA .....</b>                           | <b>3</b>  |
| <b>4. DIRETRIZES GERAIS.....</b>                      | <b>4</b>  |
| Interpretação .....                                   | 4         |
| Propriedade .....                                     | 4         |
| Classificação da Informação .....                     | 5         |
| Controle de Acesso .....                              | 5         |
| Segurança Física .....                                | 5         |
| Internet  | 6         |
| Correio Eletrônico .....                              | 6         |
| Rede Sem Fio (Wi-Fi) .....                            | 6         |
| Recursos de TIC Institucionais .....                  | 6         |
| Dispositivos Móveis Institucionais .....              | 6         |
| Recursos de TIC Particulares .....                    | 7         |
| Armazenamento de Informações.....                     | 7         |
| Repositórios Digitais .....                           | 7         |
| Mídias Sociais .....                                  | 7         |
| Mesa Limpa e Tela Limpa .....                         | 7         |
| Áudio, Vídeos e Fotos .....                           | 7         |
| Uso de Imagem, Som da Voz e Nome .....                | 8         |
| Aplicativos de Comunicação.....                       | 8         |
| Monitoramento .....                                   | 8         |
| Combate ao Preconceito e Discriminação .....          | 8         |
| Incidentes de Segurança.....                          | 8         |
| Código de Ética .....                                 | 8         |
| Boas Práticas.....                                    | 8         |
| Revisão e Atualização .....                           | 8         |
| <b>5. PAPÉIS E RESPONSABILIDADES .....</b>            | <b>9</b>  |
| Responsabilidades Gerais.....                         | 9         |
| Responsabilidades Específicas .....                   | 9         |
| <b>6. DISPOSIÇÕES FINAIS.....</b>                     | <b>10</b> |
| <b>7. DOCUMENTOS DE REFERÊNCIA .....</b>              | <b>11</b> |
| <b>APÊNDICE A – SIGLAS, TERMOS E DEFINIÇÕES .....</b> | <b>14</b> |

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

## 1. INTRODUÇÃO

A TelePuc é uma empresa de telemarketing comprometida em fornecer serviços de atendimento ao cliente de alta qualidade, valorizando a segurança e a privacidade das informações. No mundo digital altamente interconectado de hoje, garantir a proteção das informações é essencial para manter a confiança dos nossos clientes e parceiros, além de proteger os nossos ativos tangíveis e intangíveis.

Para alcançar este objetivo, a TelePuc reconhece a importância de uma gestão rigorosa e eficaz da segurança da informação. A natureza da nossa atividade, que envolve o manuseio de grandes volumes de dados pessoais e sensíveis, exige uma abordagem robusta e sistemática para prevenir incidentes que possam comprometer a integridade, a confidencialidade e a disponibilidade das informações.

Neste contexto, a segurança da informação se torna uma atividade crucial para a proteção de todos os nossos ativos, incluindo a imagem, a reputação, o patrimônio e, principalmente, a informação que é o coração das nossas operações. É vital que todos os colaboradores, independentemente de seu papel ou nível hierárquico, pratiquem e disseminem boas práticas de segurança da informação.


Em resposta a essas necessidades, estamos implementando o Sistema de Gestão de Segurança da Informação (SGSI), que tem como diretriz principal a Política de Segurança da Informação (PSI). Este sistema foi desenvolvido para atender às necessidades específicas do setor de telemarketing e garantir que nossas operações estejam em conformidade com as melhores práticas de segurança e regulamentações aplicáveis.

Para que a TelePuc alcance o objetivo de proteger seus ativos e continuar oferecendo serviços de excelência, é fundamental que todas as regras e procedimentos descritos nesta política sejam seguidos por todos os colaboradores. A colaboração e o compromisso de cada membro da equipe são essenciais para garantir um ambiente seguro e protegido para a nossa informação e a de nossos clientes.

## 2. OBJETIVOS

A Política de Segurança da Informação (PSI) da TelePuc é aplicável a todos os ambientes e operações da empresa de telemarketing, com os seguintes objetivos:

- **Estabelecer Diretrizes Estratégicas:** Definir diretrizes e princípios estratégicos para a

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

proteção de ativos tangíveis e intangíveis, como imagem, reputação, marca, propriedade intelectual, bancos de dados e conhecimento, além dos recursos de tecnologia da informação e comunicação (TIC) e das informações dos clientes.


- **Nortear a Tomada de Decisão:** Orientar a tomada de decisão e a execução das atividades profissionais de todos os colaboradores da TelePuc, em ambientes presenciais ou digitais, em conformidade com as normas internas, legislação vigente e boas práticas.
- **Promover a Segurança Operacional:** Estabelecer princípios para o desenvolvimento de operações seguras, prevenindo danos à reputação e à continuidade dos negócios da TelePuc.
- **Construir uma Cultura de Segurança:** Fomentar uma cultura de uso seguro da informação, capacitando os colaboradores a agir com responsabilidade e segurança no ambiente digital.
- **Preservar os Pilares Básicos de Segurança da Informação:** Garantir a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações e dos recursos de TIC, assegurando que os dados estejam protegidos contra acessos não autorizados, alterações indevidas e indisponibilidade.
- **Nortear Normas e Procedimentos:** Orientar a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para garantir a conformidade e a eficácia das medidas de segurança.

Esses objetivos são essenciais para assegurar que a TelePuc possa operar de maneira segura e eficiente, protegendo as informações críticas e fornecendo um serviço confiável e de alta qualidade aos nossos clientes.

### 3. ABRANGÊNCIA

Esta Política de Segurança da Informação (PSI) é um normativo interno com valor jurídico e aplicabilidade imediata e irrestrita a todos os colaboradores e prestadores de serviços da TelePuc. Ela abrange todos os ambientes operacionais e administrativos da empresa, incluindo qualquer situação em que haja acesso ou uso de informações, recursos de tecnologia da informação e comunicação (TIC), e demais ativos tangíveis ou intangíveis da TelePuc.

Esta política se aplica a:

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

1. **Todos os colaboradores:** Incluindo funcionários permanentes, temporários e terceirizados, em todos os níveis hierárquicos.

2. **Prestadores de serviços e parceiros:** Qualquer entidade externa que tenha acesso aos sistemas de informação e recursos tecnológicos da TelePuc.

3. **Ambientes operacionais e administrativos:** Qualquer local ou contexto, físico ou digital, onde as operações da TelePuc sejam realizadas e onde seus recursos e informações sejam acessados ou utilizados.

A aplicação desta política é essencial para garantir a proteção adequada das informações e ativos da TelePuc, assegurando a continuidade e a integridade dos serviços prestados.


#### 4. DIRETRIZES GERAIS

##### Interpretação

Para efeito desta Política de Segurança da Informação (PSI), são adotadas as siglas, os termos e definições constantes no Apêndice A. Esta PSI deve ser interpretada de forma restritiva, ou seja, casos excepcionais ou que não sejam por ela tratados só podem ser realizados após prévia e expressa autorização da Gerência de Segurança da Informação (GSI). Qualquer caso de exceção ou permissão diferenciada ocorrerá de forma pontual, aplicável apenas ao seu solicitante, dentro dos limites e motivos que a fundamentaram, cuja aprovação se dará por mera liberalidade da GSI e com duração limitada, podendo ser revogada a qualquer tempo e sem necessidade de aviso prévio.

##### Propriedade

As informações geradas, acessadas, recebidas, manuseadas ou armazenadas pela TelePuc, bem como a reputação, a marca, o conhecimento e demais ativos tangíveis e intangíveis, são de propriedade exclusiva da empresa. Os recursos de Tecnologia da Informação e Comunicação (TIC) fornecidos pela TelePuc para o desenvolvimento de atividades profissionais são de propriedade da empresa ou estão a ela cedidos, permanecendo sob sua guarda e posse para uso restrito e devem ser utilizados apenas para o cumprimento da finalidade a que se propõem. A utilização das marcas, identidade visual e demais sinais distintivos da TelePuc em qualquer veículo de comunicação, inclusive na internet e nas mídias sociais, só pode ser feita para atender a atividades profissionais, quando prévia e expressamente autorizada. Colaboradores podem mencionar a marca em conteúdos e materiais, para citação do local de trabalho, mas não podem criar perfis em mídias sociais em nome da instituição e/ou se fazendo passar por ela.

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

## Classificação da Informação

Para que as informações sejam adequadamente protegidas, cabe ao colaborador realizar a classificação no momento em que for gerada a informação, para garantir a devida confidencialidade, especialmente no caso de conteúdos e dados pessoais.

**Informação Pública:** Informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa qualquer dano à empresa e aos colaboradores.

**Informação Interna:** Informação que pode ser divulgada para os colaboradores da empresa, enquanto estiverem desempenhando atividades profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos institucionais.

**Informação Confidencial:** Informação exclusiva a quem se destina. Requer tratamento especial. Contém dados pessoais e/ou sigilosos que, se divulgados, podem afetar a reputação e a imagem da empresa ou causar impactos graves, sob o aspecto financeiro, legal e normativo.

**Rotulagem da Informação:** Informações não públicas devem ser rotuladas quando forem geradas, armazenadas ou disponibilizadas. Informações em mídias removíveis ou papel devem ser identificadas com carimbo, etiqueta ou texto padronizado. Para informações em ambientes lógicos, utilizar documentação específica para definir o nível de classificação.


Todos os colaboradores devem respeitar o nível de segurança requerido pela classificação indicada na informação que manusear ou com que vier a tomar contato. Em caso de dúvida, todos deverão tratar a informação como de uso interno, não passível de divulgação ou compartilhamento com terceiros ou em ambientes externos à empresa, incluindo a internet e mídias sociais, sem prévia e expressa autorização da GSI.

## Controle de Acesso

Cada colaborador recebe uma identidade digital, de uso individual e intransferível, para acesso físico e lógico aos ambientes e recursos de TIC da TelePuc. A identidade digital é monitorada e controlada pela empresa. O colaborador é responsável pelo uso e sigilo de sua identidade digital. Não é permitido compartilhá-la, divulgá-la ou transferi-la a terceiros. Todos devem estar devidamente identificados, portando o crachá individual de forma visível, enquanto estiverem nas dependências físicas da empresa. O crachá de identificação é de uso individual e não pode ser compartilhado.

## Segurança Física

A TelePuc deve estabelecer espaços físicos seguros para proteger as áreas que criam, desenvolvem, processam ou armazenam informações críticas. Os ativos críticos devem estar

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

protegidos contra a falta de energia elétrica e outras interrupções causadas por falhas, além de ter uma correta manutenção para assegurar sua contínua integridade e disponibilidade.

### **Internet**

Os recursos de conectividade são fornecidos para atender ao propósito profissional. O acesso à internet é concedido aos colaboradores por meio de identidade digital pessoal e intransferível, sendo o titular o único responsável pelas ações e/ou danos, se houver.

### **Correio Eletrônico**

A utilização do correio eletrônico corporativo deve se ater à execução das atividades profissionais, respeitando as regras de direitos autorais, licenciamento de software, direitos de propriedade e privacidade. O uso de correio eletrônico particular é permitido apenas para a transmissão ou recebimento de conteúdo ou informações particulares, sem prioridade sobre as atividades profissionais e sem efeitos negativos para a rede corporativa.

### **Rede Sem Fio (Wi-Fi)**


A TelePuc oferece rede sem fio (Wi-Fi) própria para finalidades profissionais, disponível nos ambientes autorizados e limitados ao perímetro físico da empresa. Somente os colaboradores autorizados podem ter acesso à rede sem fio e devem comprometer-se a fazer uso seguro desse recurso. Visitantes e fornecedores poderão ter acesso à rede sem fio com prévia autorização.

### **Recursos de TIC Institucionais**

Os recursos de TIC da TelePuc são destinados a finalidades estritamente profissionais. É vedado o armazenamento de arquivos pessoais nos recursos de TIC da empresa. Para a proteção das informações, os arquivos digitais devem ser armazenados nos servidores específicos, com acesso restrito. A TelePuc não se responsabiliza pelos arquivos digitais armazenados nas estações de trabalho, notebooks, tablets e smartphones disponibilizados pela empresa. Em casos de desligamento, os arquivos digitais serão apagados. Todos os recursos de TIC devem ser inventariados e identificados. Apenas é permitida a utilização de softwares e hardwares legítimos, previamente homologados ou autorizados.

### **Dispositivos Móveis Institucionais**

O uso de dispositivos móveis da TelePuc não é permitido por terceiros. Em casos de roubo, perda ou furto do dispositivo móvel institucional, o colaborador deve registrar um Boletim de Ocorrência (B.O.), entregar uma cópia do documento e notificar imediatamente o gestor e a GSI.

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

### Recursos de TIC Particulares

É vedada a conexão dos recursos de TIC particulares na rede corporativa da TelePuc. Os colaboradores autorizados podem utilizar recursos de TIC particulares conectados à rede corporativa exclusivamente para suas funções profissionais. Todos os recursos particulares devem ser protegidos com métodos de segurança, como antivírus e firewall. A TelePuc não se responsabiliza pela utilização dos softwares, arquivos digitais, suporte técnico e manutenções dos recursos de TIC particulares utilizados pelos colaboradores.

### Armazenamento de Informações

As informações da TelePuc devem ser armazenadas no local apropriado e destinado a esse fim. Informações digitais devem ser armazenadas nos servidores da rede corporativa, com controle de acesso e cópia de segurança. Informações físicas devem ser guardadas em locais seguros. A TelePuc pode solicitar a remoção de conteúdos que ofereçam riscos à empresa e seus colaboradores, sejam contrários à legislação ou possam causar danos à instituição.

### Repositórios Digitais

Os repositórios digitais para uso institucional são destinados ao armazenamento, criação, compartilhamento e transmissão de arquivos, desde que previamente autorizados. É vedado o armazenamento de arquivos pessoais nos repositórios digitais institucionais. Os repositórios para uso educacional ou acadêmico podem ser utilizados com autorização. É vedado armazenar, criar, compartilhar ou transmitir arquivos ilegais ou que comprometam a segurança da informação.

### Mídias Sociais


Os colaboradores devem adotar um comportamento seguro nas mídias sociais, em conformidade com os direitos e deveres estabelecidos. A participação institucional deve ser diretamente relacionada à função profissional e aos objetivos da empresa, sendo o colaborador responsável por suas ações e omissões.

### Mesa Limpa e Tela Limpa

Os papéis contendo informações da TelePuc não devem ficar expostos em locais públicos ou de trânsito de pessoas. Todos os colaboradores são responsáveis por realizar o bloqueio com senha ao se distanciar do recurso de TIC que estiverem usando.

### Áudio, Vídeos e Fotos

Não é permitido tirar fotos, gravar áudio, filmar, publicar e/ou compartilhar imagens da TelePuc sem prévia autorização. Situações previamente autorizadas, como eventos institucionais, são exceções. Colaboradores devem obter autorização para captar ou reproduzir imagens dentro

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

da empresa e utilizá-las apenas para fins pessoais, sem compartilhamento público.

### **Uso de Imagem, Som da Voz e Nome**

A TelePuc pode utilizar a imagem dos colaboradores para fins de identificação, autenticação, segurança, registro de atividades, uso institucional e educacional. O uso de imagem, som da voz e nome deve respeitar a integridade e reputação dos colaboradores, conforme as leis vigentes.

### **Aplicativos de Comunicação**

O uso de aplicativos de comunicação para compartilhar informações deve ser feito de forma responsável para evitar riscos à empresa. Informações institucionais devem ser compartilhadas respeitando o sigilo e as normas de segurança.

### **Monitoramento**

A TelePuc realiza o registro e monitoramento de atividades (logs) em seus ambientes físicos e lógicos, com captura de imagens, áudio ou vídeo, para proteção do patrimônio e da reputação da empresa, e para colaborar com as autoridades em caso de investigação.

### **Combate ao Preconceito e Discriminação**

Todos os colaboradores devem participar de campanhas de conscientização contra atos de preconceito e discriminação, e cooperar em situações críticas, fornecendo informações de segurança sempre que necessário.

### **Incidentes de Segurança**

Incidentes de segurança devem ser reportados imediatamente ao gestor e à GSI para investigação e adoção de medidas corretivas e preventivas.

### **Código de Ética**

Todos os colaboradores da TelePuc devem respeitar a PSI e o Código de Ética e Conduta da empresa, sendo responsáveis por suas ações e omissões.


### **Boas Práticas**

Todos devem adotar boas práticas de segurança da informação, incluindo o uso de senhas fortes, proteção dos recursos de TIC, atualização de software e hardware, além de participar de treinamentos e campanhas de conscientização.

### **Revisão e Atualização**

Esta PSI deve ser revisada e atualizada periodicamente para atender às necessidades e ao



|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

contexto da TelePuc, levando em consideração as mudanças na legislação, tecnologias e ambiente de negócio. As atualizações devem ser comunicadas a todos os colaboradores e demais interessados.

## 5. PAPÉIS E RESPONSABILIDADES


### Responsabilidades Gerais

Todos os colaboradores da TelePuc devem validar, ler e assinar a Política de Segurança da Informação no momento da contratação, garantindo que sua eficácia tenha início desde a integração do novo funcionário. O setor de Segurança da Informação (SI) é responsável por garantir a atualização da Política sempre que houver alterações ou necessidade de melhoria nos processos.

### Responsabilidades Específicas

#### Todos os Colaboradores

- **Conhecimento e Disseminação:** Conhecer e disseminar as regras e boas práticas mencionadas nesta Política.
- **Preservação e Proteção:** Preservar e proteger os ativos físicos e não físicos de propriedade ou sob a custódia da TelePuc, incluindo todas as suas informações e conteúdos, contra qualquer tipo de ameaça, como acesso, compartilhamento ou modificação não autorizados.
- **Recursos Institucionais:** Zelar pela proteção dos recursos institucionais, da marca, reputação, conhecimento e propriedade intelectual da TelePuc.
- **Uso Responsável:** Usar com responsabilidade os recursos físicos e lógicos fornecidos pela empresa.
- **Exposição de Informações:** Evitar a exposição desnecessária de informações, projetos, trabalhos e dependências da TelePuc, incluindo mídias sociais e internet, e agir com responsabilidade no uso dos recursos de TIC e das informações.
- **Prevenção de Incidentes:** Prevenir e/ou reduzir os impactos gerados por incidentes de segurança da informação, garantindo a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.
- **Conformidade:** Cumprir e manter-se atualizado com relação a esta Política, ao Regimento Interno e às demais Normas de Segurança da Informação da TelePuc.
- **Proteção de Informações:** Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados.
- **Combate a Discriminação e ao Preconceito :** Adotar medidas preventivas e reativas para

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

combater a discriminação e o preconceito, e conscientizar sobre a necessidade de coibir e conter toda forma de violência.

- **Relato de Incidentes:** Reportar imediatamente quaisquer incidentes que possam impactar na segurança das informações da TelePuc através do endereço de contato designado pela empresa.

### Gestores e Coordenadores

- **Orientação e Disseminação:** Orientar constantemente suas equipes sobre o uso seguro dos ativos tangíveis e intangíveis, e disseminar os valores adotados pela TelePuc.
- **Delegação de Funções:** Suportar todas as consequências das funções e atividades delegadas a outros colaboradores.
- **Cumprimento da Política:** Assegurar o cumprimento desta Política e das demais regulações pelos colaboradores sob sua supervisão.
- **Investigação de Incidentes:** Participar da investigação de incidentes de segurança relacionados às informações, ativos e colaboradores sob sua responsabilidade.
- **Participação no Comitê de Segurança da Informação:** Participar, sempre que convocado, das reuniões do Comitê de Segurança da Informação, prestando os esclarecimentos solicitados.


### Colaboradores

- **Sigilo e Exposição Pessoal:** Ser cauteloso quanto à exposição de sua vida particular e preservar o sigilo profissional nas mídias sociais, protegendo a imagem e reputação da TelePuc.
- **Comunicação Adequada:** Utilizar linguagem respeitosa e adequada nas comunicações, evitando termos dúbios, abusos de poder, perseguição, discriminação, assédio moral ou sexual.
- **Uso de Mídias Sociais:** Utilizar as mídias sociais de forma que evite exposição excessiva e riscos para sua própria imagem e reputação, bem como para a instituição.

## 6. DISPOSIÇÕES FINAIS

Este documento deverá ser interpretado com base nas definições disponíveis no apêndice e nas leis brasileiras.

As atitudes ou ações adversas previstas, não autorizadas ou até mesmo ilícitas baseadas nesta Política de Segurança da Informação, já serão consideradas violações. Haverá avaliação

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

pela equipe de segurança, baseado no Regimento Geral contratos de prestação de serviços, contratos de trabalho e nas demais normas da instituição, sobre o risco e a sanção específica do colaborador que descumpra a Política.

A PSI e as demais normas de segurança, incluindo folders educativos sobre como se proteger na internet, poderão ser consultados assim que solicitados para a equipe de segurança através do e-mail: [seguranca@telepuc.com.br](mailto:seguranca@telepuc.com.br), bem como estará disponível para acesso na intranet corporativa.


Em caso de eventuais dúvidas, estas devem ser mandadas por e-mail com o assunto: [DÚVIDA PSI] para: [seguranca@telepuc.com.br](mailto:seguranca@telepuc.com.br).

Em caso de dúvidas sobre possíveis phishings, potenciais incidentes, denúncias ou quebra de conduta, deverão ser encaminhados por meio do endereço: [abuse@telepuc.com.br](mailto:abuse@telepuc.com.br) ou deverão ser comunicados imediatamente para a equipe de segurança da informação via chat homologado.

## 7. DOCUMENTOS DE REFERÊNCIA

A elaboração da Política de Segurança da Informação (PSI) da TelePuc foi fundamentada em uma série de documentos de referência reconhecidos internacionalmente e alinhados com as melhores práticas de segurança da informação. Estes documentos são essenciais para garantir que a PSI esteja em conformidade com padrões, leis e regulamentações relevantes. A seguir, estão listados os principais documentos de referência utilizados:

1. **ISO/IEC 27001:2013** - Tecnologia da Informação - Técnicas de Segurança - Sistemas de Gestão de Segurança da Informação - Requisitos:
  - Esta norma especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI) no contexto dos riscos de segurança da informação gerais da organização.
2. **ISO/IEC 27002:2013** - Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação:
  - Fornece diretrizes para as melhores práticas de gestão da segurança da informação e para a implementação dos controles de segurança especificados na ISO/IEC 27001.
3. **Lei Geral de Proteção de Dados (LGPD) - Lei n.º 13.709/2018:**

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

- Regulamenta o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

4. **NIST SP 800-53** - Security and Privacy Controls for Federal Information Systems and Organizations:

- Publicação do Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos, que fornece um catálogo de controles de segurança e privacidade para todas as organizações.

5. **COBIT 5** - Control Objectives for Information and Related Technology:

- Um framework para a governança e gestão de TI da ISACA, que ajuda as organizações a criar valor a partir da TI, mantendo um equilíbrio entre a realização de benefícios e a otimização dos níveis de risco e uso de recursos.

6. **PCI-DSS** - Payment Card Industry Data Security Standard:

- Conjunto de requisitos de segurança projetado para garantir que todas as empresas que aceitam, processam, armazenam ou transmitem informações de cartão de crédito mantenham um ambiente seguro.


7. **Norma ABNT NBR ISO/IEC 27005:2011** - Tecnologia da Informação - Técnicas de Segurança - Gestão de Riscos em Segurança da Informação:

- Fornece diretrizes para a gestão de riscos em segurança da informação, suportando os requisitos do sistema de gestão de segurança da informação (SGSI) especificados na ISO/IEC 27001.

8. **Resolução n.º 4.658/2018 do Banco Central do Brasil** - Dispõe sobre a Política de Segurança Cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras.


9. **Marco Civil da Internet - Lei n.º 12.965/2014:**

- Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

#### 10. Diretivas Internas da TelePuc:

- Conjunto de políticas, normas e procedimentos internos específicos da TelePuc que complementam e detalham as diretrizes gerais da PSI.

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

## APÊNDICE A – SIGLAS, TERMOS E DEFINIÇÕES

### A

**Ameaça:** Causa potencial de um incidente indesejado que pode resultar em dano à instituição.

**Aplicativos de comunicação:** Programas de computador geralmente instalados em dispositivos móveis usados para troca rápida de mensagens, conteúdos e informações multimídia, como WhatsApp, Telegram e Snapchat.

**Ativo:** Qualquer coisa que tenha valor para a instituição e precisa ser adequadamente protegida.

**Ativos críticos:** Todos os recursos considerados essenciais para a instituição que, se não estiverem intactos, disponíveis ou acessíveis, poderão acarretar danos graves à instituição.

**Ativo intangível:** Todo elemento que possui valor para a instituição e que esteja em meio digital ou se constitua de forma abstrata, mas registrável ou perceptível, como a reputação, imagem, marca e conhecimento.

**Ativo tangível:** Bens de propriedade da instituição que são concretos e que podem ser tocados, como computadores, imóveis, móveis.

**Antivírus:** Programa de proteção do computador que detecta e elimina os vírus (programas danosos) nele existentes, assim como impede sua instalação e propagação.

**Antispyware:** Programa de proteção que detecta e elimina programas espiões (spywares) que observam e roubam informações pessoais do usuário, transmitindo-as para uma fonte externa na internet sem o conhecimento ou consentimento do usuário.


**Autenticidade:** Garantia de que as informações sejam procedentes e fidedignas, bem como capazes de gerar evidências não repudiáveis da identificação de quem as criou, editou ou emitiu.

### B

**Backup:** Salvaguarda de sistemas ou arquivos realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de retorno.

### C

**Colaborador:** Empregado, estagiário ou menor aprendiz da instituição.

|   |  |                            |
|---|--|----------------------------|
|  | <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b> | <b>PSI-001-2024</b>        |
|   |  | Versão: 1.0                |
|   | Classificação: interna                     | Última Revisão: 19/06/2024 |

## D

**Dado pessoal:** Qualquer informação relacionada a uma pessoa natural identificada ou identificável.

**Dado sensível:** Categoria especial de dados pessoais que revelem origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

## E

**Engenharia social:** Técnica usada para enganar pessoas para que revelem informações confidenciais ou realizem ações que comprometam a segurança da informação.

## I

**Incidente de segurança:** Qualquer evento que tenha potencial de comprometer a confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

**Integridade:** Propriedade que assegura que a informação não foi alterada ou destruída de maneira não autorizada.

## P

**Phishing:** Técnica de fraude em que um atacante se faz passar por uma entidade confiável para obter informações sensíveis, como senhas e dados de cartão de crédito, através de comunicações eletrônicas enganosas.

## R

**Ransomware:** Tipo de software malicioso que restringe o acesso ao sistema infectado e exige um resgate para que o acesso seja restabelecido.

## S

**Segurança da informação:** Conjunto de medidas que visam proteger a informação contra acessos não autorizados, garantindo sua confidencialidade, integridade e disponibilidade.

## T

**TelePuc:** Empresa de telemarketing especializada em serviços de atendimento ao cliente, que valoriza a segurança e a privacidade das informações.