Política de segurança da Informação

Sumário

1. OBJETIVO

Estabelecer diretrizes estratégicas para o manuseio, tratamento, controle e proteção de dados e informações sensíveis, assegurando a confidencialidade, integridade, disponibilidade e autenticidade das informações. Esta política visa fornecer orientação e suporte para a gestão da segurança da informação, garantindo a conformidade com as leis, regulamentações e melhores práticas internacionais aplicáveis. A política abrange todos os aspectos da segurança da informação, incluindo a prevenção de incidentes, a resposta a eventos de segurança, e a melhoria contínua das práticas de segurança, promovendo um ambiente seguro e resiliente para o processamento e armazenamento de informações, alinhado aos objetivos e estratégias de negócios do ITEC - Instituto de Tecnologia em Informática e Informação do Estado de Alagoas.

2. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores, prestadores de serviços, parceiros de negócios e quaisquer outros usuários que utilizem serviços e recursos tecnológicos disponibilizados e de propriedade do ITEC. Inclui todos os sistemas de informação, dispositivos, redes, processos, e dados, independentemente do formato ou localização, garantindo que as práticas de segurança sejam implementadas e seguidas de maneira consistente em toda a organização. A política abrange todas as atividades relacionadas ao tratamento e proteção da informação, incluindo, mas não se limitando a coleta, armazenamento, processamento, transmissão, e descarte de dados.

3. CONSIDERAÇÕES PRELIMINARES

A segurança da informação envolve a preservação da confidencialidade, integridade, disponibilidade e autenticidade da informação, assegurando que ela seja protegida contra acessos não autorizados, alterações indevidas e

indisponibilidade. Esta política de segurança da informação é um documento de diretrizes que, apoiado por documentos e procedimentos específicos, visa garantir a proteção das informações da organização. A política estabelece a base para a criação e manutenção de um ambiente seguro, promovendo a cultura de segurança entre todos os colaboradores e partes interessadas, e assegurando o cumprimento de requisitos legais e normativos aplicáveis.

4. PROPRIEDADE E PROTEÇÃO DA INFORMAÇÃO

Toda informação gerada, adquirida ou custodiada pelo ITEC, independentemente de sua forma de apresentação ou armazenamento, é um ativo valioso e deve ser adequadamente protegida. As informações devem ser utilizadas exclusivamente para fins relacionados aos interesses do ITEC, em conformidade com as diretrizes organizacionais e esta Política de Segurança da Informação. O ITEC se reserva o direito de monitorar o tráfego e o armazenamento de dados a qualquer momento, sem prévia notificação aos colaboradores, prestadores de serviço e demais usuários autorizados. Este monitoramento é essencial para garantir a segurança, detectar e responder a incidentes, e manter a integridade e a disponibilidade das informações.

5. PAPÉIS E RESPONSABILIDADE

5.1 Grupo de Trabalho de Segurança da Informação (GTSI)

O Grupo de Trabalho de Segurança da Informação (GTSI) no ITEC é responsável por apoiar a área de Proteção de Dados Pessoais, com foco especial na adequação à Lei Geral de Proteção de Dados (LGPD). Este grupo visa não apenas atender aos requisitos legais, mas também fortalecer a segurança de dados e práticas de privacidade.

5.2 Equipe Técnica de Tecnologia da Informação

As responsabilidades da área de Segurança da Informação no ITEC incluem, mas não se limitam a:

- **Monitoramento e Ações Corretivas**: Monitorar continuamente as violações de segurança, tomar ações corretivas imediatas e registrar todos os incidentes no sistema GLPI para garantir que não ocorram recorrências.
- **Avaliação de Vulnerabilidades**: Orientar e conduzir testes na infraestrutura de tecnologia e sistemas, visando avaliar pontos fracos e detectar possíveis vulnerabilidades e ameaças.
- **Gestão de Políticas e Procedimentos**: Revisar, publicar, manter e zelar pelas políticas e procedimentos relacionados à Segurança da Informação, além de sugerir as alterações necessárias para mantê-los atualizados e eficazes.
- **Desenvolvimento e Implantação de Controles**: Orientar o desenvolvimento, a implantação e o teste de controles técnicos e processuais de segurança da informação, garantindo que o ambiente de tecnologia permaneça seguro.
- **Treinamento e Conscientização**: Desenvolver, manter e implantar, em parceria com a área de proteção de dados pessoais, programas de treinamento e conscientização para colaboradores, prestadores de serviços e demais usuários autorizados, focando na política de segurança da informação, sua estrutura e conceitos.
- **Classificação da Informação**: Assessorar as demais áreas do ITEC no processo de classificação da informação, garantindo que os dados sejam categorizados e protegidos de acordo com sua sensibilidade.
- **Avaliação de Riscos**: Implantar programas regulares de avaliação de riscos nas áreas de negócio, oferecendo suporte contínuo aos responsáveis, especialmente quando necessário.
- **Plano de Continuidade e Disponibilidade**: Auxiliar as áreas de negócio na elaboração e manutenção do Plano de Continuidade e Disponibilidade do Negócio, assegurando que as operações possam ser retomadas rapidamente após incidentes.
- **Resposta a Incidentes**: Fornecer orientação aos recursos envolvidos para a tomada de ações rápidas em resposta a incidentes de segurança da informação detectados ou reportados.
- **Segurança no Desenvolvimento de Sistemas**: Auxiliar as áreas de desenvolvimento de sistemas desde a fase de planejamento, para

garantir que os sistemas contenham controles de segurança apropriados.

- **Práticas de Desenvolvimento Seguro**: Aplicar práticas de desenvolvimento seguro ao longo de todo o ciclo de vida do software, incluindo a identificação de vulnerabilidades, realização de testes de segurança e revisões de código.
- **Tratamento de Vulnerabilidades**: Efetuar o tratamento de vulnerabilidades identificadas de forma ágil, com planos de mitigação e correções priorizadas para minimizar os riscos.
- **Validação de Acessos**: Validar o acesso às informações de acordo com a necessidade e o nível de cada usuário, aplicando autenticação forte e atribuindo os privilégios mínimos necessários para garantir a segurança.
- **Registro de Atividades**: Manter registros detalhados de todas as atividades relevantes nos softwares, permitindo a identificação e rastreamento de ações não autorizadas.
- **Atualização de Ferramentas**: Aplicar as atualizações necessárias em ferramentas, bibliotecas e frameworks, garantindo que as últimas correções de segurança estejam em vigor.
- **Orientação para Desenvolvedores**: Orientar os desenvolvedores sobre as responsabilidades na aplicação das diretrizes de segurança e relatar prontamente eventuais vulnerabilidades identificadas durante o desenvolvimento de sistemas.

5.3 Coordenador da Segurança da Informação

O Coordenador atuará diretamente com a área de proteção de dados pessoais, liderando, coordenando e supervisionando todas as atividades pertinentes à segurança da informação para assegurar a conformidade contínua e a melhoria dos processos institucionais**.** As responsabilidades incluem, mas não se limitam a:

- Assegurar que a política de segurança da informação esteja em conformidade com os requisitos da ISO/IEC 27001 e esteja alinhada com a LGPD;
- Promover a conscientização e a capacitação contínua sobre a importância da segurança da informação e da proteção de dados pessoais em toda a organização;
- Supervisionar a avaliação, identificação e gestão dos riscos de segurança da informação;

- Garantir a eficácia e a adequação dos controles de segurança da informação para cumprir os padrões estabelecidos pelas normativas aplicáveis;
- Reportar regularmente o desempenho e os avanços ao coordenador da área de proteção de dados pessoais, assegurando transparência e alinhamento contínuo com as estratégias e regulamentações institucionais.

5.4 Gestores

Gestores no ITEC, devido à sua posição no órgão, têm a responsabilidade de garantir o cumprimento desta política de segurança da informação pelos funcionários sob sua gerência e pelos prestadores de serviço vinculados a contratos sob sua gestão. As principais responsabilidades incluem:

- **Estabelecimento de Diretrizes de Atuação**: O gestor é responsável por estabelecer claramente a forma de atuação dos colaboradores ou prestadores de serviço sob sua supervisão, assegurando que as atividades sejam realizadas em conformidade com esta política.
- **Acompanhamento e Verificação**: Cabe ao gestor acompanhar e verificar a realização das atividades dos colaboradores e prestadores de serviço, garantindo que estas estejam alinhadas com os padrões de segurança da informação do ITEC.
- **Colaboração com a Equipe de Segurança da Informação**: Sempre que necessário, o gestor deve atuar em colaboração com a equipe de Segurança da Informação, orientando e participando em processos de auditoria relacionados ao trabalho realizado pelos colaboradores e prestadores sob sua supervisão.
- **Gerenciamento de Acessos e Privilégios**: É responsabilidade do gestor informar, através de chamado formal, a necessidade de concessão, modificação ou remoção de privilégios e acessos dos colaboradores aos sistemas utilizados no Instituto. Essa comunicação garante que os acessos estejam sempre alinhados às necessidades reais e às políticas de segurança do ITEC.

5.5 Administrativo

É responsabilidade da área administrativa aplicar os controles de acesso físico às dependências do Instituto, abrangendo tanto funcionários quanto visitantes. As principais atividades incluem:

- **Controle de Acesso para Funcionários**: Garantir que todos os funcionários possuam os devidos credenciais e autorizações para acessar as áreas do Instituto, de acordo com suas funções e necessidades operacionais.
- **Gestão de Visitantes**: Implementar e monitorar rigorosos procedimentos de controle de acesso para visitantes, incluindo a emissão de credenciais temporárias e a restrição de acesso às áreas específicas, conforme a finalidade de sua visita.

5.6 Colaboradores, Prestadores de Serviço e Demais Usuários Autorizados

Os colaboradores, prestadores de serviço e demais usuários autorizados a acessar e utilizar as informações do ITEC desempenham um papel crucial na Segurança da Informação. Suas atividades diárias fornecem dados e insights valiosos para os agentes de segurança da informação do ITEC, contribuindo diretamente para a proteção dos ativos informacionais da empresa.

Todos esses indivíduos devem estar plenamente comprometidos com o manuseio e a utilização adequada das informações e dos recursos computacionais disponibilizados pela organização, seguindo rigorosamente as diretrizes e procedimentos estabelecidos. A adesão a essas práticas é fundamental para manter a integridade, confidencialidade e disponibilidade das informações do ITEC.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações geradas, adquiridas ou custodiadas pelo ITEC devem ser classificadas de acordo com sua sensibilidade e necessidade de proteção. A classificação permite garantir que as informações sejam protegidas de maneira adequada, de acordo com seu nível de criticidade e valor para a organização. As informações do ITEC serão classificadas nas seguintes categorias:

- **Pública**: Informações que podem ser disponibilizadas e acessíveis para consulta irrestrita por qualquer pessoa, sem impacto negativo sobre a organização.
- **Interna**: Informações que são destinadas ao uso interno do Instituto e que, se divulgadas externamente, podem causar danos à reputação ou ao desempenho operacional do ITEC.

- **Confidencial**: Informações sensíveis que são restritas a setores específicos do Instituto. O acesso a essas informações devem ser rigorosamente controladas, e qualquer divulgação não autorizada pode resultar em danos significativos à organização.
- **Restrita**: Informações de alta sensibilidade, acessíveis apenas a indivíduos específicos e com necessidade clara para realizarem suas funções. A divulgação não autorizada dessas informações pode causar danos severos e irreparáveis ao ITEC.

Todas as informações, enquanto não devidamente classificadas e divulgadas de forma oficial, devem ser tratadas como "Reservadas", e a classificação adequada deve ser aplicada o mais rapidamente possível para assegurar a proteção adequada.

6.1 Tratamento da Informação

Os colaboradores, prestadores de serviço e demais usuários autorizados não estão autorizados a realizar cópias para uso pessoal ou divulgação das informações do ITEC - Instituto de Tecnologia em Informática e Informação, a menos que tenham recebido autorização expressa da alta gestão.

- **Informações Confidenciais e Restritas**: Não podem ser acessadas ou copiadas para mídias ou ambientes externos, incluindo a Internet, sem a devida autorização da alta gestão. Essas informações devem ser armazenadas de forma segura, preferencialmente criptografadas, nos servidores do ITEC.
- **Manuseio e Armazenamento Seguro**: Todas as informações devem ser manuseadas e armazenadas de forma segura, conforme as diretrizes de classificação. Quando não mais necessárias, as informações devem ser adequadamente descartadas, seguindo as políticas de classificação e de tratamento de informações.
- **Descarte de Informações**: No descarte de informações em formato físico (papel), os documentos devem ser triturados e descartados conforme as diretrizes da Política de Mesa Limpa e Tela Limpa. Da mesma forma, os dispositivos de armazenamento de rede, como discos rígidos, devem ser tratados conforme as políticas de reformatação e descarte seguro, garantindo que nenhuma informação sensível permaneça acessível.

7. SEGURANÇA FÍSICA E DO AMBIENTE

A segurança física e do ambiente é fundamental para proteger as informações e os ativos do ITEC. O controle de acesso físico às instalações e áreas sensíveis é essencial para evitar acessos não autorizados e proteger a integridade dos dados e sistemas.

7.1 Acesso Físico

Todo o acesso às instalações do ITEC deve ser rigorosamente controlado. A responsabilidade pelo fornecimento e controle de crachás para colaboradores e prestadores de serviço recai sobre o setor Administrativo e as empresas prestadoras de serviço contratadas. A segurança e portaria do ITEC, sob a gestão do setor Administrativo, são responsáveis por monitorar e controlar o acesso de todas as pessoas que circulam nas dependências do instituto, assegurando que visitantes recebam o crachá ou etiqueta de identificação correspondente, com acesso limitado às áreas específicas necessárias para sua função ou visita.

- **Áreas de Acesso Restrito**: O acesso à Diretoria de Serviço de Tecnologia da Informação e Telecomunicação, bem como ao Datacenter, deve ser autorizado apenas pela alta gestão, diretores ou gerentes do setor. Para clientes, o acesso ao Datacenter é rigorosamente controlado e registrado via chamado no sistema GLPI.
- **Identificação e Controle**: Todos os colaboradores, prestadores de serviço e visitantes são obrigados a se identificar prontamente quando solicitados pela portaria. Apenas colaboradores e prestadores de serviço autorizados podem permitir a entrada de visitantes, e somente quando essa entrada for relevante para os interesses do ITEC. Em caso de extravio de crachá, o ocorrido deve ser imediatamente comunicado ao setor de Valorização de Pessoas.
- **Segurança e Vigilância**: O responsável pela administração do ITEC deve ser informado imediatamente sobre a presença de qualquer pessoa não identificada, não autorizada ou visitante desacompanhado. O acesso às áreas onde são processadas ou armazenadas informações sensíveis é restrito ao pessoal técnico autorizado e à equipe técnica do ITEC. Equipamentos de gravação ou fotografia não são permitidos nessas áreas sem autorização expressa.
- **Documentação e Transferência de Itens**: Qualquer movimentação de itens pertencentes ao ITEC deve ser devidamente documentada no sistema de patrimônio vigente. Se o item pertencer a um cliente, a

transferência deve ser registrada via chamado, incluindo a anuência do cliente e, quando aplicável, registro fotográfico.

- **Atividades que Afetam Recursos de TI**: Qualquer atividade que possa impactar o funcionamento dos recursos de TI do ITEC deve ser previamente autorizada e realizada por pessoal capacitado. Consultas ao gestor administrativo e/ou ao gestor de TI são necessárias para assegurar que as atividades sejam conduzidas de maneira segura e eficaz.

8. ZELO DAS INFORMAÇÕES

A proteção e o zelo pelas informações são fundamentais para garantir a segurança e a integridade dos dados no ITEC. Todas as informações confidenciais e restritas devem ser manuseadas com o mais alto nível de cuidado e responsabilidade.

8.1 Manuseio e Armazenamento de Informações

Informações classificadas como confidenciais ou restritas não devem, em hipótese alguma, ser deixadas desprotegidas sobre mesas de trabalho, dentro de gavetas ou armários sem chave. Este cuidado deve ser estendido a qualquer material impresso, que não deve ser deixado em bandejas de impressoras ou em áreas acessíveis a indivíduos não autorizados.

- **Cloud Pública**: É estritamente proibido armazenar informações de propriedade do ITEC, classificadas como confidenciais e/ou restritas, em ambientes de cloud pública. Qualquer necessidade de armazenamento externo deve ser previamente aprovada e realizada de forma segura, conforme as diretrizes da organização.
- **Proteção de Estações de Trabalho**: Ao se ausentar de sua estação de trabalho, mesmo que por um breve período, o colaborador deve proteger o acesso ao computador utilizando senhas de acesso, garantindo que a informação permanece segura contra acessos não autorizados.

8.2 Desenvolvimento de Projetos de Software

Todos os desenvolvimentos de projetos de software e colaborações relacionados ao ITEC devem ser hospedados exclusivamente nos repositórios de projetos designados pela área de desenvolvimento de sistemas. É absolutamente proibido hospedar qualquer projeto ou código institucional em repositórios pessoais, como GitHub ou Bitbucket, a menos que haja uma autorização prévia do gestor da área de desenvolvimento de sistemas.

- **Controle de Acesso aos Repositórios**: O acesso aos repositórios de projetos de software da instituição deve ser rigorosamente controlado e concedido apenas a membros da equipe ou colaboradores autorizados, de acordo com suas funções e necessidades específicas. Esse controle é essencial para proteger a propriedade intelectual do ITEC e garantir que as informações sejam acessadas e manipuladas apenas por pessoas devidamente autorizadas.

9. MESA LIMPA E TELA LIMPA

A política de Mesa Limpa e Tela Limpa é essencial para proteger as informações sensíveis do ITEC contra acessos não autorizados, perdas e outras ameaças. Esta política garante que as informações confidenciais e restritas sejam mantidas seguras, tanto fisicamente quanto digitalmente, em todas as estações de trabalho e áreas de trabalho.

9.1 Mesa Limpa

Informações confidenciais ou restritas nunca devem ser deixadas desprotegidas sobre mesas de trabalho, dentro de gavetas ou armários que não estejam trancados. Este cuidado deve ser estendido a qualquer material impresso, que não deve ser deixado nas bandejas das impressoras ou em áreas acessíveis a pessoas não autorizadas.

- **Armazenamento Seguro**: Todos os documentos e materiais sensíveis devem ser armazenados em locais seguros, como gavetas ou armários trancados, ao final do expediente ou sempre que o colaborador se ausentar de sua mesa, mesmo que por um curto período.

9.2 Tela Limpa

Quando o usuário se ausentar de sua estação de trabalho, mesmo que por um breve período, ele deve proteger o acesso ao computador utilizando senhas ou bloqueio de tela. Esta medida assegura que informações sensíveis não sejam acessadas por pessoas não autorizadas.

- **Configuração de Bloqueio Automático**: As estações de trabalho devem ser configuradas para trancar a sessão do usuário automaticamente após 10 (dez) minutos de inatividade. Esta regra se aplica tanto para recursos locais quanto para recursos remotos, garantindo uma camada adicional de proteção.

9.3 Verificação e Auditoria

Para garantir o cumprimento desta política, poderão ser realizadas verificações periódicas, como rondas ou auditorias, para assegurar que a política de Mesa Limpa e Tela Limpa está sendo seguida corretamente. Essas verificações podem incluir a observação de mesas desocupadas para verificar se estão limpas e se todas as informações sensíveis estão devidamente guardadas, bem como o monitoramento do uso correto das funções de bloqueio de tela.

10. EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

O uso de equipamentos particulares e dispositivos móveis no ambiente de rede do ITEC é controlado para garantir a segurança das informações e a integridade dos sistemas. Somente colaboradores e prestadores de serviço devidamente autorizados podem conectar dispositivos móveis, como notebooks, à rede do ITEC, e isso deve ser feito de acordo com os requisitos estabelecidos.

10.1 Autorização e Uso de Equipamentos

A utilização de notebooks pessoais ou outros dispositivos móveis para acessar a rede do ITEC só será permitida mediante uma solicitação justificada e aprovação prévia. Os dispositivos autorizados devem estar em

conformidade com as políticas de segurança do ITEC, incluindo atualizações em dia de sistemas operacionais, antivírus e a ausência de programas obsoletos ou com falhas de segurança.

- **Requisitos de Segurança**: Sob nenhuma circunstância devem ser executados nos dispositivos móveis conectados à rede do ITEC softwares maliciosos ou programas que possam comprometer a comunicação e a segurança do Instituto. Dispositivos que violarem essas regras poderão ter seus endereços MAC bloqueados sem prévio aviso.
- **Responsabilidade do Proprietário**: É de responsabilidade do proprietário do equipamento garantir que somente softwares legalizados sejam utilizados em seu dispositivo. O armazenamento de informações pertencentes ao ITEC em dispositivos móveis pessoais é estritamente proibido.

10.2 Armazenamento e Transferência de Informações

Os arquivos de propriedade intelectual e informações classificadas como restritas ou privadas não podem ser armazenados em discos rígidos de notebooks pessoais ou em dispositivos de armazenamento móvel, como pendrives ou armazenamento em nuvem pessoal. O ITEC dispõe de soluções de nuvem privada para armazenamento seguro dessas informações.

- **Proibição de Pendrives**: O uso de pendrives no Instituto é proibido e controlado por regras de domínio. A cópia de informações privadas ou restritas para dispositivos móveis externos ao Instituto será restrita e só permitida em situações estritamente necessárias, sempre seguindo o fluxo de autorização.

10.3 Responsabilidades e Boas Práticas

Cabe à área de TI do ITEC implementar e divulgar mecanismos que maximizem a segurança dos equipamentos utilizados no ambiente do Instituto. Os colaboradores são responsáveis por zelar pelos equipamentos sob sua guarda, garantindo que estes sejam manuseados exclusivamente para atender aos interesses da instituição, conforme descrito nesta política.

11. GERENCIAMENTO DO AMBIENTE COMPUTACIONAL

O gerenciamento eficaz do ambiente computacional é crucial para garantir a segurança, integridade e disponibilidade dos recursos de TI. Todas as operações envolvendo conexões de rede, configurações de sistema, proteção contra software malicioso, e respostas a incidentes de segurança são conduzidas de acordo com as diretrizes estabelecidas.

11.1 Conexões de Redes

A conexão de qualquer equipamento à rede interna do ITEC só pode ser realizada por representantes autorizados da empresa. Somente colaboradores, prestadores de serviço e parceiros de negócios devidamente autorizados têm permissão para acessar a rede do ITEC.

- **Acesso Remoto**: Acessos remotos à rede do ITEC, exceto para serviços públicos, devem ser autorizados e só são permitidos para atividades diretamente relevantes ao negócio do Instituto. Esses acessos devem ser realizados por meio de VPN disponibilizada pelo ITEC, conforme os requisitos de segurança estabelecidos.
- **Conexões Seguras:** A conexão de prestadores de serviço ou parceiros, tanto no modo local quanto remoto, é permitida desde que sejam garantidos todos os requisitos de segurança conforme as Políticas de Acesso à Rede, que são verificadas e avaliadas pela área de Segurança da Informação.
- **Computadores Externos**: Computadores não pertencentes ao ITEC só podem ser conectados à rede do Instituto após autorização da gestão de TI e cumprimento das políticas e configurações de segurança. O ITEC se reserva o direito de auditar esses equipamentos para garantir a segurança das informações.

11.2 Senhas

As senhas são o método mais comum de autenticação de usuários e são essenciais para proteger a identidade do servidor e os recursos do ITEC.

- **Regras de Criação de Senhas**: As senhas de autenticação na rede devem ter um mínimo de 8 caracteres, incluir letras, números, ao menos uma letra maiúscula, e, de preferência, caracteres especiais. As

senhas devem ser fáceis de lembrar para o usuário, mas não óbvias ou baseadas em informações pessoais (como datas de aniversário).

- **Manutenção e Confidencialidade**: As senhas devem ser mantidas em segredo, não compartilhadas, e alteradas a cada 90 dias. O compartilhamento de logins para funções de administração de sistemas é proibido. As senhas não devem ser anotadas e deixadas próximas ao computador.

11.3 Alterações de Configuração

Colaboradores, prestadores de serviço ou usuários autorizados não podem realizar alterações nas configurações dos recursos computacionais do ITEC. Toda e qualquer alteração deve ser conduzida pelos representantes autorizados do Instituto, conforme as diretrizes estabelecidas pela área de TI.

11.4 Uso da Internet

A internet é uma ferramenta de trabalho no ITEC, e seu uso é restrito a atividades profissionais que estejam em conformidade com as normas legais e éticas. O acesso a sites de conteúdo impróprio, como pornografia, discriminação racial, ou atividades ilegais, é estritamente proibido.

11.5 Proteção contra Software

Todo computador conectado à rede do ITEC, seja de forma local ou remota, deve ter obrigatoriamente instalado, atualizado e ativado um software de proteção contra vírus.

- **Medidas de Segurança com Softwares**: É proibida a instalação de softwares sem autorização prévia. Apenas softwares devidamente licenciados podem ser utilizados. A utilização de software não licenciado constitui uma infração legal, conforme previsto na Lei nº 9.609/1998. Qualquer remoção ou modificação de software ou hardware sem a devida autorização pode comprometer a segurança e o desempenho da estação de trabalho.

11.6 Cópias de Segurança

Os representantes autorizados do ITEC são responsáveis por realizar regularmente o backup das informações mantidas nos servidores do Instituto, conforme a política de backup interna. Os arquivos armazenados nas estações de trabalho não serão incluídos em rotinas de backup, como ocorre com as pastas de rede de setores ou usuários.

11.7 Uso do Correio Eletrônico

O uso do correio eletrônico no ITEC é regido pela Política de Segurança de E-mail, que deve ser seguida por todos os colaboradores e prestadores de serviço.

11.8 Uso de Criptografia

Somente é permitida a utilização de mecanismos de criptografia homologados e autorizados pelo ITEC, e apenas nos casos previamente aprovados.

11.9 Incidentes de Segurança da Informação

Incidentes de Segurança da Informação são definidos como quaisquer eventos adversos, suspeitos ou confirmados, que possam comprometer a integridade, confidencialidade ou disponibilidade das informações ou serviços do ITEC. Exemplos incluem:

- Mau funcionamento de sistemas ou serviços;
- Ataques, como engenharia social ou negação de serviço;
- Acesso não autorizado;
- Envio ou recebimento de códigos maliciosos;
- Alterações em sistemas sem aprovação.

12. RECURSOS DE INFORMÁTICA

A gestão e utilização adequada dos recursos de informática do ITEC são essenciais para manter a segurança, integridade e funcionalidade dos sistemas de TI. Este item define as diretrizes para a instalação, configuração e movimentação de software e hardware dentro do ambiente institucional.

12.1 Instalação e Configuração de Software e Hardware

A utilização de software ou hardware nos recursos computacionais de propriedade do ITEC é estritamente limitada a itens que tenham sido homologados, licenciados e controlados pelo Instituto. A instalação e configuração desses recursos são responsabilidades exclusivas dos representantes autorizados do ITEC.

- **Software e Hardware Homologados**: Somente softwares e hardwares que passaram pelo processo de homologação e licenciamento pelo ITEC podem ser utilizados em seus recursos computacionais. Isso garante que todos os componentes instalados estejam em conformidade com os padrões de segurança e operacionais da organização.
- **Responsabilidade pela Instalação**: A instalação e configuração de qualquer software ou hardware devem ser realizadas exclusivamente por representantes autorizados do ITEC. Prestadores de serviço externos podem realizar essas tarefas apenas com o suporte e sob a supervisão do ITEC, e somente em recursos computacionais pertencentes ao Instituto.
- **Recursos Computacionais Custodiados**: No caso de recursos computacionais que foram alocados ou custodiados por parceiros ou prestadores de serviços, esses também devem ser homologados pelo ITEC, e suas configurações devem ser gerenciadas exclusivamente por representantes autorizados.

12.2 Movimentação de Recursos de Informática

A movimentação de qualquer recurso computacional de propriedade do ITEC deve ser realizada apenas por representantes autorizados da área de TI do Instituto.

- **Autorização para Movimentação**: Somente os representantes autorizados têm permissão para mover recursos computacionais dentro do ITEC. No entanto, os usuários podem, sob a orientação e supervisão da equipe de suporte, mover equipamentos que estão sob sua guarda direta, garantindo que essas movimentações sejam realizadas de maneira segura e conforme as políticas do Instituto.

13. CONTROLE DE ACESSO LÓGICO

O controle de acesso lógico é um elemento fundamental para garantir que as informações e recursos do ITEC sejam acessados apenas por usuários devidamente autorizados, minimizando o risco de acessos não autorizados e garantindo a proteção dos dados e sistemas críticos da organização.

13.1 Princípios de Acesso

Colaboradores, prestadores de serviço e demais usuários autorizados devem ter acesso apenas às informações e recursos necessários para a realização de suas atividades, respeitando sempre o princípio de segregação de funções.

- **Segregação de Funções**: Atribuir acessos de forma que as responsabilidades e permissões sejam claramente delineadas evita conflitos de interesse e minimiza o risco de fraudes ou abusos.
- **Violação de Segurança**: Tentar acessar qualquer serviço de TI ou informação sem a devida autorização, burlar as restrições de segurança, prejudicar um serviço de informação, interceptar comunicação de forma não autorizada, ou utilizar os recursos do ITEC para atividades maliciosas constitui grave violação da Política de Segurança da Informação e será tratada com seriedade.

13.2 Controle de Acesso e Auditoria

Todos os sistemas do ITEC devem possuir controles de acesso robustos, garantindo que apenas usuários autorizados possam utilizá-los. Sistemas críticos devem, adicionalmente, registrar trilhas de auditoria (logs) que possibilitem o monitoramento e rastreamento das atividades executadas.

- **Logs de Auditoria**: A implementação de trilhas de auditoria nos sistemas críticos permite que todas as ações dos usuários sejam monitoradas, ajudando na detecção de atividades suspeitas e na investigação de incidentes de segurança.

13.3 Movimentações de Pessoal e Atualizações de Acesso

As movimentações de pessoal, como admissões, transferências, promoções e demissões, devem ser comunicadas ao departamento administrativo, que providenciará as atualizações necessárias no ambiente computacional.

- **Gestão de Acesso para Contratados**: Para recursos humanos alocados através de contratos, cabe aos gestores de contratos com fornecedores, ou seus representantes designados, solicitar permissões, renovações e cancelamento de acessos para os prestadores de serviço. Caso não ocorra a renovação, o acesso desses usuários será automaticamente bloqueado.

- **Procedimentos de Desligamento**: No caso de desligamento de um colaborador, o acesso às contas deve ser imediatamente bloqueado, e os dados armazenados em correio eletrônico e servidores de arquivos devem ser tratados de acordo com a Política de Segurança de E-mail do órgão.

13.4 Permissões de Acesso e Responsabilidades

As permissões de acesso, concebidas e implantadas pela área de TI, são únicas e intransferíveis. Cada usuário é responsável por todas as ações realizadas através de sua conta de acesso.

- **Responsabilidade do Usuário**: Todo usuário deve manter sua conta de acesso segura e não compartilhar suas credenciais com terceiros. Qualquer atividade realizada sob a conta do usuário é de sua responsabilidade, e qualquer uso indevido pode resultar em sanções conforme as políticas do ITEC.

14. PLANO DE CONTINUIDADE OPERACIONAL

O Plano de Continuidade Operacional é um componente essencial para garantir que os recursos computacionais e os serviços de TI do ITEC possam continuar operando, ou ser rapidamente restabelecidos, em caso de interrupções ou desastres. Este plano é fundamental para a resiliência da organização e para a minimização dos impactos negativos em suas operações.

14.1 Responsabilidade pela Elaboração e Atualização

A equipe de Segurança da Informação, com o apoio da gestão de TI, é responsável por coordenar a elaboração, atualização e implementação do Plano de Continuidade Operacional. Esse plano deve cobrir todos os aspectos críticos dos recursos computacionais de TI, assegurando que os procedimentos para recuperação e continuidade estejam claramente definidos e sejam eficazes.

- **Elaboração do Plano de Continuidade Operacional**: A equipe de Segurança da Informação deve identificar os processos críticos e os recursos tecnológicos necessários para a operação contínua do ITEC.

Com base nessas informações, o plano deve ser elaborado para abordar diferentes cenários de interrupção, desde falhas técnicas até desastres naturais.

- **Atualização Contínua**: O plano de continuidade operacional não é um documento estático; ele deve ser revisado e atualizado regularmente para refletir mudanças nos recursos de TI, nas operações da organização, e nas ameaças e riscos identificados.

14.2 Testes Periódicos

É essencial que o Plano de Continuidade Operacional seja testado periodicamente para garantir sua eficácia. Esses testes permitem identificar possíveis falhas no plano e ajustar os procedimentos antes que um incidente real ocorra.

- **Simulações e Exercícios**: A equipe de Segurança da Informação deve realizar simulações e exercícios regulares para testar diferentes partes do plano, incluindo a recuperação de sistemas críticos e a restauração de dados. Os resultados desses testes devem ser documentados e utilizados para aprimorar o plano.
- **Envolvimento da Gestão de TI**: A gestão de TI deve estar envolvida em todos os testes do plano, garantindo que as estratégias de continuidade estejam alinhadas com as capacidades e as limitações dos recursos tecnológicos disponíveis.

14.3 Documentação e Melhoria Contínua

Todos os aspectos do Plano de Continuidade Operacional, incluindo os resultados dos testes e quaisquer revisões, devem ser documentados de forma detalhada. A documentação é crucial para a transparência e a melhoria contínua do plano.

- **Registro Detalhado**: Cada teste, simulação ou atualização do plano deve ser registrado, incluindo os procedimentos seguidos, os resultados observados, e as ações corretivas implementadas. Essa documentação facilita a auditoria e a revisão do plano, assegurando que ele permaneça eficaz ao longo do tempo.
- **Ciclo de Melhoria Contínua**: Com base na documentação e nos resultados dos testes, o plano deve ser continuamente aprimorado para refletir as melhores práticas e responder às novas ameaças e desafios que surgem no ambiente de TI.

15. CONFORMIDADE

A conformidade com as diretrizes organizacionais, políticas internas e regulamentações externas é essencial para garantir que o ITEC opere de maneira segura, ética e em conformidade com todas as obrigações legais e contratuais. Este item reforça o compromisso do ITEC com a conformidade em todos os níveis da organização, abrangendo colaboradores, prestadores de serviço, parceiros de negócios e demais usuários autorizados.

15.1 Adesão às Diretrizes e Regulamentos

Todos os colaboradores, prestadores de serviço e demais usuários autorizados do ITEC devem aderir não apenas às Diretrizes Organizacionais e à Política de Segurança da Informação, mas também a todas as leis, estatutos, regulamentos e contratos aplicáveis à organização.

- **Cumprimento de Normas e Leis**: O compromisso com a conformidade inclui a observância de todas as leis e regulamentações relevantes, garantindo que as operações do ITEC estejam sempre em conformidade com os padrões legais exigidos.
- **Obrigações Contratuais**: Além das leis e regulamentos, todos os contratos celebrados pelo ITEC devem ser cumpridos rigorosamente, respeitando todas as cláusulas e condições acordadas com clientes, fornecedores e parceiros.

15.2 Auditorias e Verificações de Conformidade

Para garantir que o ITEC e todos os envolvidos em suas operações estejam em conformidade com as diretrizes e regulamentos, é necessário realizar auditorias periódicas. Essas auditorias ajudam a identificar e corrigir qualquer desvio das normas estabelecidas.

- **Recursos e Informações para Auditorias**: O ITEC deve disponibilizar todos os recursos e informações necessários para a realização eficaz de auditorias periódicas. Isso inclui acesso a registros, sistemas e quaisquer dados relevantes que possam ser necessários para verificar a conformidade.
- **Acompanhamento das Auditorias**: Após a realização das auditorias, os resultados devem ser cuidadosamente analisados, e quaisquer não conformidades devem ser tratadas com ações corretivas para assegurar a plena conformidade contínua.

15.3 Cláusulas de Confidencialidade em Contratos

Todos os contratos realizados pelo ITEC, seja como contratante ou contratado, devem incluir cláusulas específicas de confidencialidade para proteger as informações trocadas entre as partes.

- **Confidencialidade com Parceiros de Negócios**: Nos contratos com parceiros de negócios, além das cláusulas de confidencialidade, deve-se assegurar que os acordos estejam em conformidade com todas as regulamentações aplicáveis à proteção de dados e segurança da informação.
- **Proteção da Informação**: Essas cláusulas de confidencialidade são essenciais para garantir que todas as informações compartilhadas com parceiros e fornecedores sejam devidamente protegidas contra acessos não autorizados e uso indevido.

16. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação do ITEC deve ser rigorosamente seguida por todos os colaboradores, prestadores de serviço e demais usuários autorizados. A violação desta política pode resultar em sanções disciplinares, conforme descrito abaixo, e será tratada de acordo com a legislação trabalhista e a gravidade da infração.

16.1 Procedimentos em Caso de Violação

Ao identificar ou suspeitar de uma possível violação da Política de Segurança da Informação, é obrigatório que o colaborador ou usuário busque orientação imediata com o Gestor da área. O Gestor, em conjunto com a Equipe de Segurança da Informação, é responsável por apurar os fatos e tomar as medidas necessárias.

- **Notificação de Incidentes**: Todos os colaboradores, prestadores de serviço e usuários autorizados devem notificar imediatamente o Gestor da área e ao Coordenador da Segurança da Informação sobre qualquer fragilidade, ameaça, incidente ou suspeita de violação que comprometa a segurança de sistemas, controles ou serviços.
- **Restrições de Investigação**: Não é permitido, sob nenhuma circunstância, que qualquer colaborador ou usuário tente averiguar

uma falha de segurança ou uma atividade suspeita por conta própria. A investigação de vulnerabilidades ou incidentes deve ser conduzida exclusivamente pela Equipe de Segurança da Informação, evitando assim o uso impróprio dos sistemas ou informações.

16.2 Classificação das Infrações e Sanções

As infrações à Política de Segurança da Informação são classificadas em três categorias: Leve, Média e Grave. As sanções correspondentes são aplicadas de acordo com a gravidade da infração e a legislação aplicável.

- **Infração Leve**:
  - **Sanção**: O colaborador recebe uma notificação por e-mail com cópia para o Gestor da área. A falta não é registrada na pasta funcional do colaborador.
- **Infração Média**:
  - **Sanção**: O colaborador recebe uma notificação escrita do gestor imediato, e a ocorrência é registrada na pasta funcional do colaborador.
- **Infração Grave**:
  - **Sanção**: O colaborador recebe uma notificação escrita do gestor imediato, e a ocorrência é registrada na pasta funcional. A situação será submetida à análise da Alta Direção do ITEC para definição das providências adicionais.
- **Reincidência**: Em caso de reincidência, a infração será considerada no próximo grau de escala. Por exemplo, duas infrações leves relacionadas à mesma matéria constituem uma infração média.

17. GERENCIAMENTO DE MUDANÇAS

O Gerenciamento de Mudanças é um processo crucial para garantir a estabilidade, segurança e continuidade dos serviços no ambiente de TI do ITEC. Todas as mudanças, sejam elas no ambiente físico ou computacional, devem ser rigorosamente controladas para mitigar riscos e assegurar que os serviços continuem a ser entregues com eficiência, minimizando impactos adversos nos negócios.

17.1 Controle de Mudanças

Toda mudança no ambiente de TI do ITEC, que possa impactar a infraestrutura física ou os sistemas computacionais, deve ser cuidadosamente planejada e controlada. Isso inclui alterações em hardware, software, redes, políticas de segurança e qualquer outro componente que possa afetar a operação normal dos serviços.

- **Processo de Aprovação**: Antes de implementar qualquer mudança, é necessário realizar um estudo prévio de impacto e risco como parte do Procedimento de Gestão de Mudanças. Este estudo deve considerar os efeitos da mudança em termos de segurança, continuidade dos negócios, e impacto nos clientes internos e externos.
- **Documentação das Mudanças**: Todas as mudanças devem ser documentadas detalhadamente, incluindo o motivo da mudança, o plano de implementação, os riscos identificados, as medidas de mitigação e o resultado esperado. Essa documentação é essencial para auditorias e para futuras referências em caso de problemas.

17.2 Mitigação de Riscos

O objetivo principal do Gerenciamento de Mudanças é mitigar os riscos associados a qualquer alteração no ambiente de TI. Isso inclui garantir que as mudanças não comprometam a segurança, a disponibilidade ou a integridade dos sistemas e serviços do ITEC.

- **Análise de Risco**: Cada mudança proposta deve passar por uma análise de risco detalhada, que inclui a identificação de potenciais problemas, a avaliação de sua probabilidade e impacto, e a definição de estratégias de mitigação.
- **Planos de Contingência**: Para mudanças de alto impacto, devem ser desenvolvidos planos de contingência que possam ser acionados em caso de falha na implementação da mudança. Esses planos garantem que, mesmo que algo dê errado, a continuidade do negócio não seja comprometida.

17.3 Continuidade dos Negócios

A continuidade do negócio é uma prioridade em qualquer processo de mudança. O Gerenciamento de Mudanças deve assegurar que as operações

do ITEC possam continuar de forma eficiente, mesmo durante a implementação de alterações significativas no ambiente de TI.

- **Monitoramento e Validação Pós-Mudança**: Após a implementação de qualquer mudança, é essencial realizar um monitoramento contínuo para validar os resultados e garantir que a mudança tenha alcançado os objetivos previstos sem introduzir novos problemas.
- **Feedback e Melhoria Contínua**: Com base nas lições aprendidas durante o processo de mudança, deve-se buscar a melhoria contínua dos procedimentos de gestão de mudanças, ajustando práticas e políticas conforme necessário para melhor atender às necessidades do ITEC.

18. SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LEI Nº 13.709/2018)

A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece diretrizes essenciais para o tratamento de dados pessoais, e todos os colaboradores, prestadores de serviço e usuários dos serviços prestados pelo ITEC devem seguir rigorosamente os princípios desta lei. A conformidade com a LGPD é fundamental para proteger os direitos dos titulares de dados e para assegurar que o ITEC opere dentro dos parâmetros legais estabelecidos.

18.1 Princípios Fundamentais

Todos os colaboradores diretos e indiretos, bem como os usuários dos serviços do ITEC, devem pautar suas ações pelos princípios fundamentais da LGPD, que orientam o tratamento de dados pessoais, assegurando a proteção dos direitos dos titulares e a conformidade com a legislação. Os princípios a seguir devem ser observados em todas as atividades de tratamento de dados pessoais:

- **Finalidade**: Os dados pessoais devem ser tratados para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
- **Adequação**: O tratamento de dados deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento.

- **Necessidade**: O tratamento deve se limitar ao mínimo necessário para a realização de suas finalidades, abrangendo apenas os dados pertinentes, proporcionais e não excessivos.
- **Livre Acesso**: Os titulares dos dados têm o direito de acessar e consultar, de forma gratuita e facilitada, os dados pessoais que lhes dizem respeito e as informações relacionadas ao seu tratamento.
- **Qualidade dos Dados**: Os dados pessoais devem ser exatos, claros, relevantes e atualizados de acordo com a necessidade e para o cumprimento da finalidade do tratamento.
- **Transparência**: O tratamento de dados deve ser realizado de forma clara e acessível, garantindo que os titulares sejam informados sobre os aspectos relevantes do tratamento, como as finalidades, os critérios e os procedimentos utilizados.
- **Segurança**: Medidas técnicas e administrativas devem ser adotadas para proteger os dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.
- **Prevenção**: Medidas proativas devem ser implementadas para prevenir a ocorrência de danos decorrentes do tratamento de dados pessoais, visando a proteção contínua dos titulares.
- **Não Discriminação**: Os dados pessoais não podem ser utilizados para fins discriminatórios, ilícitos ou abusivos, assegurando que o tratamento respeite a dignidade e os direitos dos titulares.
- **Responsabilização e Prestação de Contas**: O ITEC deve adotar medidas eficazes para demonstrar a conformidade com as normas de proteção de dados pessoais e estar preparado para prestar contas sobre suas práticas de tratamento, garantindo a transparência e a confiança dos titulares.

18.2 Procedimentos para Casos Omissos

Em situações em que a aplicação dos princípios da LGPD não estiver claramente definida, ou em casos omissos, é necessário que esses sejam remetidos para análise do(a) Encarregado(a) de Dados (Data Protection Officer - DPO) do ITEC.

- **Função do Encarregado(a) de Dados**: O Encarregado(a) de Dados é o profissional responsável por garantir que as operações do ITEC estejam em conformidade com a LGPD, assegurando a aplicação adequada dos princípios de proteção de dados e a implementação do compliance relacionado à privacidade.

- **Consulta e Análise**: Colaboradores e usuários devem consultar o Encarregado(a) de Dados sempre que houver dúvidas sobre a aplicação da LGPD, ou quando surgirem situações não previstas explicitamente nas diretrizes do ITEC.

18.3 Conformidade e Responsabilidade

É responsabilidade de todos os envolvidos garantir que os dados pessoais sejam tratados conforme as diretrizes da LGPD, e qualquer desvio ou suspeita de não conformidade deve ser reportado imediatamente ao Encarregado(a) de Dados para avaliação e correção.

- **Ações Corretivas**: O Encarregado(a) de Dados, ao identificar não conformidades, deve tomar as medidas corretivas necessárias para alinhar as práticas do ITEC aos requisitos legais, promovendo a proteção dos dados pessoais em todos os níveis operacionais.

19. AUDITORIA DA POLÍTICA

A auditoria regular da Política de Segurança da Informação é essencial para assegurar que todas as diretrizes estabelecidas estão sendo rigorosamente seguidas e aplicadas dentro do ITEC. Essas auditorias garantem a conformidade contínua com a política e identificam áreas onde melhorias podem ser necessárias.

19.1 Realização de Auditorias

A área de Serviços de Tecnologia da Informação e Telecomunicação é responsável por conduzir auditorias periódicas para verificar, por amostragem, se todos os itens desta política estão sendo cumpridos. As auditorias são realizadas sem aviso prévio, a fim de garantir a integridade e a eficácia do processo de verificação.

- **Auditoria por Amostragem**: As auditorias serão realizadas por amostragem, o que permite uma verificação representativa das práticas e procedimentos adotados no ITEC, sem a necessidade de revisar todos os casos individualmente.
- **Sem Aviso Prévio**: A realização de auditorias sem aviso prévio assegura que os processos e práticas sejam avaliados em seu estado natural,

garantindo uma avaliação mais precisa da conformidade com a política.

19.2 Participação Obrigatória

Todos os colaboradores que forem selecionados para participar da auditoria estão obrigados a colaborar plenamente com o processo. Recusar-se a participar ou obstruir a auditoria de qualquer forma constitui uma violação da Política de Segurança da Informação e pode resultar em sanções disciplinares.

- **Cooperação do Colaborador**: O colaborador auditado deve fornecer todas as informações e acesso necessários ao auditor para que a verificação seja realizada de forma completa e eficiente.
- **Consequências da Não Conformidade**: Qualquer recusa em participar da auditoria, ou a tentativa de obstruir o processo, será tratada como uma infração grave, sujeita às sanções previstas na política e na legislação aplicável.

19.3 Avaliação e Ação Corretiva

Após a realização da auditoria, os resultados serão avaliados pela área de Serviços de Tecnologia da Informação e Telecomunicação. Quaisquer não conformidades identificadas serão documentadas e deverão ser corrigidas prontamente.

- **Documentação dos Resultados**: Os resultados da auditoria devem ser cuidadosamente documentados, incluindo detalhes sobre quaisquer desvios observados e as ações corretivas recomendadas.
- **Implementação de Melhorias**: Com base nos resultados da auditoria, a equipe responsável deve implementar as ações corretivas necessárias para alinhar as práticas do ITEC com as diretrizes estabelecidas na política, promovendo a melhoria contínua da segurança da informação.

20. HISTÓRICO DAS REVISÕES

Revisão	Descrição das alterações	Data
00	Emissão Inicial	04/10/2021

01	Ajustes gerais	07/01/2022
02	Ajustes Gerais e inserção do item 19	24/11/2023
03	Revisão geral	12/08/2023

Elaborado por: Juliano Araújo Farias	Data da Elaboração: 04/10/2021
Revisado por: Alcimeire Alessandra Costa Araújo	Data de Revisão: 12/08/2023
Aprovado por: Adolfo Henrique Bernardes de Castro	Data de aprovado por: 13/08/2023