SUMÁRIO

1. OBJETIVO

Definir diretrizes estratégicas no manuseio, tratamento, controle dos dados, informações classificadas e sensíveis, e conhecimentos produzidos, armazenados ou transmitidos com o propósito de garantir à confidencialidade, integridade, disponibilidade e autenticidade para prover e estabelecer a orientação e apoio para a gestão de segurança da informação de acordo com as leis e regulamentações normativas alinhadas ao negócio do ITEC - Instituto de Tecnologia em Informática e Informação.

2. ABRANGÊNCIA

Todos os colaboradores que utilizam serviços e recursos tecnológicos disponibilizados e de propriedade do ITEC - Instituto de Tecnologia em Informática e Informação, incluindo terceiros, parceiros de negócios e prestadores de serviços.

3. CONSIDERAÇÕES PRELIMINARES

3.1 Segurança da Informação trata-se da preservação da confidencialidade, disponibilidade, integridade e legalidade da informação.

3.2 Política de segurança da informação é um documento de diretrizes apoiado por manuais e procedimentos, visando garantir a Segurança da Informação da empresa.

4. PROPRIEDADE E PROTEÇÃO DA INFORMAÇÃO

Toda a informação gerada, adquirida ou custodiada pelo ITEC - Instituto de Tecnologia em Informática e Informação, independente da forma de apresentação ou armazenamento, é importante ativo da empresa e deve ser adequadamente protegida.

As informações devem ser utilizadas exclusivamente para fins relacionados aos interesses do ITEC - Instituto de Tecnologia em Informática e Informação, observando as orientações contidas nas diretrizes organizacionais e desta Política de Segurança da Informação, sendo facultado o ITEC - Instituto de Tecnologia em Informática e Informação monitorar a qualquer momento, o tráfego e armazenamento de dados sem prévia notificação aos colaboradores, prestadores de serviço e demais usuários autorizados conforme descrito no termo de compromisso, sigilo e anuência.

5. PAPÉIS E RESPONSABILIDADE

5.1 Comitê de Segurança da Informação

Dentro das dependências do ITEC o responsável é o Gestor de TI do ITEC, e composto por um ou mais integrantes do ITEC e no mínimo duas pessoas do órgão-cliente, dos quais deverá ter poder de decisão sob a estrutura organizacional do órgão-cliente, quando aplicável, e que poderá definir:

5.1.1 Estabelecer diretrizes e aprovar as políticas e procedimentos relacionados à Segurança da Informação;

5.1.2 Designar, definir ou alterar as atribuições da estrutura de Segurança da Informação;

5.1.3 Garantir que a segurança seja parte do processo de planejamento;

5.1.4 Aprovar e suportar as principais iniciativas de Segurança da Informação para melhoria contínua das medidas de proteção visando minimizar os riscos identificados;

5.1.5 Direcionar os esforços e recursos propostos pela área de Segurança da Informação conforme a estratégia de negócios e de Tecnologia da Informação (TI);

5.1.6 Acompanhar incidentes reportados pela área de Técnica, e;

5.1.7 Atuar como fórum de discussão e tratar outros aspectos de segurança não contemplados pela Política de Segurança da Informação.

5.2 Equipe Técnica de TI

Algumas das atividades da área de Segurança da Informação incluem, mas não se limitam a:

5.2.1 Monitorar as violações de segurança, tomar ações corretivas e registrar em GLPI para assegurar que não haja recorrência;

5.2.2 Orientar testes da infraestrutura de tecnologia e de sistemas para avaliar pontos fracos e detectar possíveis vulnerabilidades e ameaças;

5.2.3 Revisar, publicar, zelar e manter as políticas e procedimentos relacionados à Segurança da Informação e sugerir as alterações necessárias;

5.2.4 Orientar o desenvolvimento, a implantação e o teste dos controles técnicos e processuais de segurança da informação necessários para garantir a segurança do ambiente de tecnologia;

5.2.5 Desenvolver, manter e implantar em parceria com a área Administrativa, programas de treinamento e conscientização aos colaboradores, prestadores de serviços e demais usuários autorizados sobre a política de segurança da informação, bem como sua estrutura e seus conceitos;

5.2.6 Assessorar as demais áreas do ITEC em Soluções Tecnológicas no processo de classificação da informação;

5.2.7 Implantar programas regulares de avaliação de riscos nas áreas de negócio, auxiliando os responsáveis destas, sempre que necessário;

5.2.8 Auxiliar as áreas de negócio na elaboração do Plano de Continuidade e Disponibilidade do Negócio;

5.2.9 Fornecer orientação aos recursos envolvidos para a tomada de ações rápidas caso sejam detectados e/ou alertados para incidentes de segurança da informação;

5.2.10 Auxiliar áreas de desenvolvimento de sistemas durante a fase de planejamento a fim de que estes contenham controles de segurança.

5.2.11 Aplicar práticas de desenvolvimento seguro ao longo de todo o ciclo de vida do software, incluindo a identificação de vulnerabilidades, testes de segurança e revisões de código.

5.2.12 Efetuar o tratamento de vulnerabilidades identificadas de forma ágil, com planos de mitigação e correções priorizadas.

5.2.13 Validar o acesso às informações consoante a necessidade e nível de cada usuário. A autenticação forte deve ser aplicada, e privilégios mínimos necessários devem ser atribuídos.

5.2.14 Manter registros de todas as atividades relevantes nos Softwares, permitindo a identificação de ações não autorizadas.

5.2.15 Aplicar atualizações necessárias de ferramentas, bibliotecas e frameworks com as últimas correções de segurança.

5.2.16 Orientar os desenvolvedores sobre as responsabilidades da aplicação das diretrizes de segurança e relatar eventuais vulnerabilidades.

5.3 Gestores ITEC

Colaboradores que, devido a sua posição na empresa, são responsáveis por garantir o cumprimento desta política para funcionários sob sua gerência ou prestadores de serviço vinculados a contratos sob sua gestão. Devido a sua responsabilidade, fica atrelado ao gestor, estabelecer a forma de atuação do colaborador ou prestador de serviço, bem como seu acompanhando e verificação da realização do seu(s) trabalho(s) e quando necessário atuar, colaborar, orientar e identificar junto com a equipe de Segurança da Informação nos casos de auditoria do trabalho(s) realizados(s).

Informar através de chamado para garantir privilégios, acessos ou remoções dos colaboradores aos sistemas utilizados no Instituto.

5.4 Administrativo

Aplicar os controles de acesso as dependências do Instituto, tanto para funcionários quanto para visitantes.

5.5 Colaboradores, prestadores de serviço e demais usuários autorizados

Os colaboradores, prestadores de serviço e demais usuários autorizados a usar informações da companhia, configuram-se em importante elo da Segurança da Informação. Com base em suas atividades fornecem subsídios para os agentes de segurança da informação do ITEC em Soluções Tecnológicas e devem estar comprometidos com o manuseio e utilização adequada das informações e recursos computacionais oferecidos pela empresa.

6. CLASSIFICAÇÃO DA INFORMAÇÃO

As informações do ITEC em Soluções Tecnológicas devem ser classificadas em uma das seguintes categorias: pública, interna, confidencial e restrita. Todas as Informações, enquanto não devidamente classificadas e divulgadas de forma oficial, são consideradas reservadas, com base na classificação:

- Público: Informações que podem ser disponibilizadas e acessíveis à consulta irrestrita a qualquer pessoa.
- Restrito: Informações disponibilizados apenas a setores do Instituto;
- Privado: Informações de acesso restrito a colaboradores do Instituto.

6.1 Tratamento da Informação

Aos colaboradores, prestadores de serviço e demais usuários, não é permitido realizar cópias para uso pessoal ou divulgação das informações do ITEC - Instituto de Tecnologia em Informática e Informação.

Informações confidenciais não podem ser acessadas ou copiadas para mídias, e para ambientes externos (incluindo a Internet) sem a devida autorização da alta gestão ou da direção, elas ficarão armazenadas e podendo estar criptografadas nos servidores do ITEC.

As Informações devem ser manuseadas e armazenadas de forma segura e adequadamente descartadas quando não mais necessárias conforme a de Classificação descrita no item 6.0, e Tratamento de Informações, definido em informação documentada abaixo.

No momento do descarte de qualquer informação, quando esta estiver em forma de papel, este(s) deve(m) ser triturados e descartados, obedecendo à Política de Mesa Limpa e Tela Limpa descrita no item 9.0, o mesmo quando se referir aos dispositivos de rede como disco rígido (por exemplo, pelo motivo de reformatação de equipamento), estes deverão atender às descritas no Tratamento da Informação seguindo a Política de Classificação.

7. SEGURANÇA FÍSICA E DO AMBIENTE

7.1 Acesso Físico

Todo o acesso deve ser controlado. Caberá ao Administrativo e a empresa prestadora, o fornecimento e controle de crachá de colaboradores e prestadores de serviço. Cabe à portaria/segurança pertencente ao setor Administrativo controlar o acesso de pessoas que circulam nas dependências do ITEC, fornecendo aos visitantes o respectivo crachá ou etiqueta de identificação, que deve segregar o seu acesso às áreas específicas, de acordo com a função ou finalidade de sua presença.

Acesso a Diretoria de Serviço de Tecnologia da Informação e Telecomunicação devem ser liberadas apenas com anuência da alta gestão, diretor ou gerentes do setor, acesso ao Datacenter por clientes é controlado via chamado no GLPI.

É responsabilidade dos colaboradores e prestadores de serviço se identificarem, quando solicitado, para a Portaria do Itec e zelar pela proteção de acesso às diversas áreas da empresa. Apenas colaboradores do Instituto e prestadores de serviço autorizados podem permitir a entrada de visitantes, quando relevante para os interesses do órgão.

Em caso de extravio de crachá deve-se comunicar imediatamente ao Recursos Humanos local.

O responsável pela administração do ITEC - Instituto de Tecnologia em Informática e Informação deve ser informado sobre a presença de qualquer pessoa não identificada, não autorizada ou de qualquer visitante não acompanhado, considerando-se sempre as permissões de acesso específicas para as diversas dependências do Instituto.

Não é permitida a utilização de equipamento de gravação ou de fotografia, sem autorização, em áreas com informações confidenciais ou em centro de processamento de informações.

O acesso às áreas em que são processadas ou armazenadas informações sensíveis é restrito apenas ao pessoal técnico autorizado e à equipe técnica do ITEC.

É obrigatório que todos os servidores, estagiários, fornecedores e todos os visitantes, tenham alguma forma visível de identificação.

Para a transferência de qualquer item pertencente ao órgão de informática, será necessário documentar a mudança junto ao sistema de patrimônio vigente, quando pertencente ao cliente deverá ser registrado em chamado com anuência e registro fotográfico quando pertinente.

Atividades que possam afetar o funcionamento dos recursos de TI do ITEC devem ser autorizadas e executadas por pessoa capacitada, assim como manipular ou remover qualquer recurso. Deve-se consultar o gestor administrativo e/ou o gestor de TI.

8. ZELO DAS INFORMAÇÕES

Informações confidenciais ou restritas não devem ser deixadas sobre a mesa de trabalho, dentro de gaveta ou armário sem chave. Cuidados semelhantes se aplicam ao material impresso deixado nos escaninhos/bandejas de impressoras.

É expressamente proibido que informações de propriedade do Itec classificadas como confidenciais e/ou restritas fiquem em ambiente de cloud pública. Ao ausentar-se de sua estação, mesmo que por breve período, o colaborador deve protegê-la de acessos com senha de acesso.

Todo desenvolvimento de software, projetos e colaborações relacionados à instituição devem ser hospedados exclusivamente nos repositórios de projetos definidos pela Diretoria de Desenvolvimento do ITEC. Tornando estritamente proibido hospedar qualquer projeto ou código institucional em repositórios pessoais, a exemplo do GitHub, Bitbucket, salvo previamente autorizado pela Diretoria de Desenvolvimento.

O acesso aos repositórios de projetos da instituição deve ser estritamente controlado e concedido apenas a membros da equipe ou colaboradores autorizados, de acordo com suas funções e necessidades.

9. MESA LIMPA E TELA LIMPA

Não deve ser deixada sobre a mesa de trabalho, dentro de gaveta ou armário sem chave informação confidencial ou restrita. Cuidados semelhantes se aplicam ao material impresso e deixado nos escaninhos de impressoras da empresa.

Ao ausentar-se de sua estação de trabalho mesmo que por breve período, o usuário deve protegê-la de acessos indevidos com senha de acesso. As estações de trabalho devem estar configuradas para trancar a sessão do usuário depois de 5 minutos de ociosidade (Esta regra se aplica para os recursos locais e remotos).

Poderá ser efetuada uma verificação (ronda), para efeito de auditagem, por exemplo, se a mesa e tela limpa, encerramento de sessão, gavetas trancadas, estão sendo cumpridas.

10. EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

A utilização de equipamentos particulares e dispositivos móveis no ambiente de rede só será permitida para realizar atividades no ITEC seguindo os requisitos de aprovação. Apenas colaboradores e prestadores de serviço, devidamente autorizados, poderão conectar o computador móvel.

A liberação para utilização de notebooks e para acesso à internet do ITEC/AL se dará mediante solicitação justificada.

O uso de notebooks particulares para fins de acesso à rede de Internet do ITEC, deverá ter suas atualizações em dia, incluindo sistema operacional, antivírus, evitando uso de programas obsoletos com falhas de segurança.

Sob hipótese alguma poderão ser executados nos notebooks, computadores switchs, roteadores ligados a rede, software de característica maliciosa, que visam comprometer o funcionamento da comunicação do órgão, podendo ter seu endereço de MAC bloqueado dentro do Instituto sem prévio aviso.

É de responsabilidade do proprietário usar somente softwares legalizados em seu notebook ou computador pessoal.

É proibido o armazenamento de informações de propriedade do ITEC.

Os arquivos de propriedade intelectual que pertencem ao ITEC e possuem dados classificados como restrito ou privado, não poderão ser armazenados no disco rígido do notebook e/ou em dispositivos de armazenamento móvel, como por exemplo: pendrive e/ou armazenamento em nuvem pessoal. O Instituto dispõe de nuvem privada.

O uso de pendrive é proibido no Instituto, sendo bloqueada com regras de domínio.

A cópia de informações privada ou restrita para trânsito extra órgãopara dispositivos móveis será restrita, devendo obedecer ao fluxo de autorização, e devendo ser permitida apenas quando estritamente necessária.

Cabe à área de TI implantar e divulgar mecanismos que maximizem a segurança dos equipamentos.

Cabe ao colaborador zelar pelo equipamento sob sua guarda, devendo manuseá-lo atendendo exclusivamente aos interesses da instituição conforme descrito neste item.

11. GERENCIAMENTO DO AMBIENTE COMPUTACIONAL

11.1 Conexões de Redes

A conexão de quaisquer equipamentos à rede interna do ITEC - Instituto de Tecnologia em Informática e Informação somente deve ser realizada pelos representantes autorizados da empresa e por eles conduzida. Somente colaboradores prestadores de serviço e parceiros de negócios, devidamente autorizados, podem ter acesso à rede do Itec.

Acessos remotos à rede da ITEC, excetuando-se acessos a serviços públicos, devem ser autorizados, sendo estes apenas para atividades relevantes para o negócio da empresa e utilizando VPN disponibilizada pelo ITEC e adequado aos requisitos de segurança.

É permitida a conexão de prestadores de serviço ou parceiros na rede da empresa, tanto no modo local quanto no modo remoto, desde que sejam garantidos os requisitos de segurança, conforme as Políticas de Acesso à rede, os quais são verificados e avaliados pela área de Segurança da Informação.

Computadores não pertencentes ao ITEC só podem ser conectados à rede do Instituto quando autorizados pela gestão de TI depois de executados às políticas e configurações de segurança. O Instituto poderá auditar os equipamentos de prestadores de serviço ou parceiros para garantir a segurança de sua informação.

Colaboradores terão acesso única e exclusivamente àqueles recursos da rede corporativa que lhe forem indispensáveis à realização de suas atividades.

É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe de suporte ao usuário através de chamado.

O ITEC disponibilizará o acesso à rede de internet sem fio (wi-fi) a seus colaboradores, o ingresso na rede se dará mediante usuário do AD já cadastrado. O acesso dos visitantes se dará mediante a geração de um token. A rede de internet sem fio (wi-fi) será segregada, garantindo assim o isolamento da rede interna.

11.2 Senha

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do servidor, evitando que uma pessoa, se faça passar por outra. O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 - falsa identidade). Com o objetivo de orientar a criação de senhas seguras, ficam estabelecidas as seguintes regras:

- Tamanho mínimo da senha de autenticação na rede é de 08 caracteres;
- Deverá ter letras, números e ao menos uma letra maiúscula;
- De preferência com caracteres especiais;
- Não óbvia, de fácil identificação;
- Fácil para o usuário lembrar;
- Proibido o uso de informações pessoais (aniversário, nome e etc...);
- Mantida em segredo e não compartilhada;

As senhas de acesso à rede de computadores e aos sistemas informatizados devem ser alteradas, a cada 90 (noventa) dias.

Fica proibido o compartilhamento de “login” para funções de administração de sistemas.

As senhas sob hipótese alguma devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.).

11.3 Alterações de Configuração

O colaborador, prestador de serviço ou usuário autorizado não pode realizar alterações nas configurações dos recursos computacionais do ITEC. Toda alteração deve ser conduzida pelos representantes autorizados do Instituto.

11.4 Internet

A Internet é uma ferramenta de trabalho, não sendo permitido seu uso para acesso a sites de conteúdos considerados impróprios ou fora dos padrões adotados pela empresa, ou seja, conteúdos que não estejam em conformidade com as normas legais, a moral, a integridade e os bons costumes, tais como os relativos à: pornografia, obscenidades, discriminação racial, política, terrorismo etc.

11.5 Proteção contra Software

Todo computador conectado à rede do ITEC - Instituto de Tecnologia em Informática e Informação, de forma local ou remota, deve ter obrigatoriamente instalado, atualizado e ativado software de proteção contra vírus.

Assim recomendamos algumas medidas de segurança que devem ser adotadas quanto à utilização de softwares:

- Não sejam instalados softwares sem a autorização;
- Só sejam utilizados softwares devidamente licenciados;
- A utilização de software não licenciado ou considerado “pirata” constitui infração prevista na Lei no 9.609/1998;
- Fica proibido remover ou modificar qualquer software, ou hardware sem a autorização da área de Tecnologia do ITEC, pois, tal atitude pode comprometer a segurança e o desempenho da estação de trabalho;

11.6 Cópias de Segurança

Cabe aos representantes autorizados a realizarem regularmente o backup de informações mantidas nos servidores do Instituto conforme política de backup interno.

Os arquivos dispostos nas estações de trabalho não serão inclusos em eventuais rotinas de backup como acontece com as pastas de rede de setores ou usuários.

11.7 Uso do Correio Eletrônico

Disposto na Política de Segurança de E-mail.

11.8 Uso de Criptografia

Apenas é permitida a utilização de mecanismos de criptografia homologados e somente nos casos autorizados pelo ITEC.

11.9 Incidentes de Segurança da Informação

Incidentes de Segurança da Informação são todos e quaisquer eventos adversos, sob suspeita ou confirmados que possam comprometer as informações ou um ativo de informação ou serviços, que tem sua integridade, confidencialidade ou disponibilidade comprometida. Como incidentes de segurança, podemos citar:

- Mau funcionamento de sistemas ou serviços;
- Ataques (como os de engenharia social ou de negação de serviço);
- Acesso não autorizado;
- Envio ou recebimento de códigos maliciosos;
- Alterações em um sistema sem a aprovação do proprietário e perda;
- Toda e qualquer ação que for contra a Política de Segurança da Informação do ITEC, também deve ser tratada como um incidente de segurança.

Os incidentes relacionados a ataques de agentes ao DC/ITEC deverão ser tratados primeiramente por bloqueios e proteção de filtros de segurança, em seguida notificação através de e-mail ao responsável técnico de TI do cliente.

12. RECURSOS DE INFORMÁTICA

12.1 Instalação e Configuração de Software e Hardware

Em recursos computacionais de propriedade do ITEC somente é permitida a utilização de software ou hardware homologado, licenciado e controlado pelo Instituto. É restrito apenas para os representantes autorizados, a instalação e configuração de software ou hardware em qualquer recurso computacional de propriedade da ITEC - Instituto de Tecnologia em Informática e Informação.

Recursos computacionais custodiados (alocado etc.) devem ser homologados pela empresa e, apenas seus representantes autorizados podem instalar e configurar software e hardware. Aos prestadores de serviço o suporte atenderá somente recursos computacionais do ITEC - Instituto de Tecnologia em Informática e Informação.

12.2 Movimentação de Recursos de Informática

Somente representantes autorizados da TI podem movimentar recursos computacionais de propriedade do ITEC - Instituto de Tecnologia em Informática

e Informação. Sendo permitido, adicionalmente, que usuários através da equipe de suporte movimentam computadores sob sua guarda.

13. CONTROLE DE ACESSO LÓGICO

O colaborador, prestador de serviço e demais usuários autorizados devem ter acesso somente às informações e recursos que forem necessários para a realização de suas atividades devendo ser respeitada a segregação de funções. Constitui-se grave violação da Política de Segurança da Informação tentar acessar qualquer serviço de TI ou informação sem a devida autorização, tentar burlar as restrições de segurança, tentar prejudicar serviço de informação, interceptar comunicação de forma não autorizada ou utilizar os recursos do ITEC - Instituto de Tecnologia em Informática e Informação para atividade maliciosa.

Todo sistema deve possuir controle de acesso de modo a assegurar o uso apenas por usuário autorizado, e sistemas críticos devem permitir o registro de trilhas de auditoria (logs) que possibilitem o monitoramento das atividades executadas.

As movimentações de pessoal (admissão, transferência, promoção, demissão) devem ser comunicadas para o administrativo, que providenciará as atualizações necessárias no ambiente computacional. Cabe ao gestor do colaborador garantir que a Gestão de Recursos Humanos tenha conhecimento destas movimentações. Para os recursos humanos alocados através de contratos, cabe aos gestores de contratos com fornecedores, ou seus representantes designados, solicitar permissões, renovações e cancelamento de acessos aos prestadores de serviço decorrentes destes contratos. Não ocorrendo renovação o acesso destes usuários será bloqueado.

Em caso de desligamento, o acesso é bloqueado e os dados armazenados no correio eletrônico e servidor de arquivos serão tratados de acordo com a Política de Segurança de E-mail do órgão.

As permissões de acesso (login ou conta), concebidas e implantadas pela área de TI, são únicas e intransferíveis. É de responsabilidade do usuário qualquer ação executada através de sua conta de acesso.

14. PLANO DE CONTINUIDADE OPERACIONAL

Cabe à equipe de Segurança da Informação, apoiada pela gestão de TI, coordenar a elaboração, atualização e testes periódicos de Plano de Continuidade para os recursos computacionais de TI da organização.

15. CONFORMIDADE

O ITEC - Instituto de Tecnologia em Informática e Informação, seus colaboradores, prestadores de serviço e demais usuários autorizados devem submeter-se não

somente às Diretrizes Organizacionais e à Política de Segurança da Informação, mas também a qualquer lei, estatuto, regulamento ou contrato a qual esteja sujeita a organização.

Devem ser disponibilizados recursos e informações que permitam a realização periódica de auditorias.

Os contratos efetuados pelo ITEC - Instituto de Tecnologia em Informática e Informação como contratante ou contratada, deve sempre constar uma cláusula de confidencialidade das informações. Para os casos de parceiros de negócios, deverá conter em contrato as conformidades e cláusulas de confidencialidade das informações trocadas.

16. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A violação a esta política, está sujeita às sanções disciplinares, passíveis de punições conforme abaixo descritas, e em conformidade com a legislação trabalhista e a gravidade da infração.

Ao identificar ou suspeitar de possível violação da Política de Segurança da Informação, deve-se buscar orientação com o Gestor da área, que, juntamente com a Equipe de Segurança da Informação, deverá apurar os fatos.

Os colaboradores, prestadores de serviço e demais usuários autorizados devem notificar imediatamente para o Gestor da área e para a equipe de Segurança da Informação, quaisquer fragilidades, ameaças ou incidentes ocorridos ou suspeitos, na segurança de sistemas, em controles ou serviços. Não é permitido, sob nenhuma circunstância, tentar averiguar uma falha de segurança ou uma atividade suspeita, pois a investigação de uma fragilidade pode ser interpretada como uso impróprio do sistema ou da informação, estando tais averiguações restritas à Equipe de Segurança.

Infração:

Leve: Notificação por e-mail para o colaborador com cópia para o gestor, não sendo a falta registrada na pasta funcional dele.

Média: Notificação escrita pelo gestor imediato e a ocorrência registrada na pasta funcional do colaborador.

Grave: Notificação escrita pelo gestor imediato e a ocorrência registrada na pasta funcional do colaborador. Análise da Alta Direção do ITEC para providências.

Em caso de reincidência, a infração deve ser considerada no próximo grau de escala. Ex.: Duas faltas leves referentes à mesma matéria constituem falta média.

17. GERENCIAMENTO DE MUDANÇAS

O Gerenciamento da mudança é fundamental no ambiente, onde toda a mudança deve ser controlada, mitigando riscos e garantindo a disponibilidade de serviços, entrega de resultados aos clientes e a continuidade do negócio no ambiente produtivo, sendo assim e quando aplicável toda alteração ou mudança que possa interferir no ambiente físico ou computacional será motivo de estudo prévio no Procedimento de Gestão de Mudanças.

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

Todos os colaboradores diretos ou indiretos, bem como os usuários dos serviços prestados pelo ITEC, devem atuar pautados pelos princípios da LGPD – especialmente a finalidade, adequação e necessidade, visando ao atendimento dos parâmetros definidos pelo órgão. Os casos omissos, deverão ser remetidos para análise do(a) Encarregado(a) de Dados do órgão, profissional responsável a garantir a aplicação do compliance e leis de proteção aos dados.

19. AUDITORIA DO POLÍTICA

Em tempos oportunos a Diretoria de Serviços de Tecnologia da Informação e Telecomunicação irá realizar por amostragem se todos os itens desta política estão sendo atendidos, sem prévio aviso, ao colaborador que estiver sendo auditado não poderá se recusar.

20. HISTÓRICO DE ATUALIZAÇÃO

Data	Revisão	Descrição	Responsável
04/10/2021	00	Emissão Inicial	Juliano Araújo Farias
07/01/2022	01	Ajustes gerais	Juliano Araújo Farias
24/11/2023	02	Ajustes Gerais e inserção do item 19	Felipe Gomes Athayde

21. ELABORAÇÃO, REVISÃO E APROVAÇÃO

	NOME	CARGO
Elaboração	Juliano Araújo Farias	Diretor
Revisão	Felipe Gomes Athayde	Gerente
Aprovação	Juliano Araújo Farias	Diretor