

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O QUE É E QUAIS SEUS OBJETIVOS?

É o conjunto de padrões, normas e diretrizes que estabelece princípios, compromissos, valores, requisitos e orientações a fim de mitigar riscos para os dados armazenados em organizações públicas e privadas. Todos aqueles que trabalham para alguma em qualquer tipo de negócio, empresa ou organizações têm normas a seguir para garantir a segurança das informações corporativas.

Pensando nisso, o CIETEC elaborou a Política de Segurança da Informação e Proteção de Dados com o objetivo garantir a segurança da informação no âmbito interno e conscientizar os colaboradores sobre o tema, através de princípios, orientações e conceitos, bem como, quais são as diretrizes trazidas pela lei.

Assim, além do mencionado acima, fornece uma camada adicional de proteção para os dados sensíveis de uma organização que realiza o armazenamento de tais dados, sendo muito importante trabalhar com as boas práticas internas. Inclusive quando são dados de informações confidenciais, financeiras, saúde ou dados de clientes.

Uma política de segurança da informação é um documento oficial que inclui informações e regras sobre a gestão de senhas, acesso a dados, acesso ao ambiente virtual interno, gerenciamento de dispositivos móveis, boas práticas de equipamentos de trabalhos usuais como notebooks e computadores e outras questões correlatas.

OBJETIVO

- Estabelecer diretrizes e normas que permitam aos colaboradores, prestadores de serviços e terceiros do CIETEC seguir padrões de comportamento desejáveis e aceitáveis, de acordo com a legalidade e as boas práticas mundiais, a fim de mitigar riscos técnicos e jurídicos;
- Assegurar o treinamento contínuo e atualizado das políticas e dos procedimentos de Segurança da Informação, enfatizando as obrigações das pessoas em relação à respectiva segurança;
- Nortear a definição de procedimentos específicos de Segurança da Informação e a implementação de controles e processos para o atendimento de seus requisitos;
- Preservar a confidencialidade, a integridade e a disponibilidade das informações do CIETEC;
- Prevenir possíveis incidentes e responsabilidade legal da instituição e de seus colaboradores, prestadores de serviços e terceiros;
- Garantir a normalidade e a continuidade das atividades do CIETEC, protegendo de momentos de crise contra falhas ou riscos importantes ;
- Minimizar os riscos de danos, perdas financeiras, participação no mercado, confiança de clientes e de parceiros ou qualquer outro impacto negativo nas atividades do CIETEC resultante de uma falha de segurança ou vazamento de dados;

A quem a lei se aplica?

Esta política deverá ser de conhecimento de todos os colaboradores da organização, independente do grau hierárquico. Não apenas a equipe de Tecnologia da Informação de uma empresa que deve se submeter a este controle, mas toda a estrutura organizacional, uma vez que a utilização massiva de tecnologia faz com que todos os dados informacionais sejam compartilhados com quem precisa trabalhar com eles.

PRINCIPAIS CONCEITOS

Ativo: todo e qualquer bem do CIETEC que possui valor econômico, incluindo a informação, e todo o recurso utilizado para o seu tratamento, tráfego e armazenamento.

Ativo Crítico e Sensível: todo ativo considerado essencial para o CIETEC, cujo acesso por pessoas não autorizadas ou a falta de acesso por quem é permitido podem causar danos à instituição.

Cavalo de Tróia (Trojan horse): programa malicioso que cria abertura para outros programas e invasões indesejadas.

Código Executável: arquivo interpretado pelo computador como um comando de execução para determinadas funções.



Código Malicioso: programa que possibilita ações danosas, como vírus, worms, trojans, spywares, malware, botnet, ransomware, entre outros.

Colaborador Interno: qualquer pessoa que execute atividade profissional e que possua algum tipo de contrato de trabalho com o CIETEC (Exemplos: funcionários e estagiários).

Colaborador Externo: qualquer pessoa contratada por empresa terceirizada que execute alguma atividade profissional nas dependências do CIETEC, sem vínculo empregatício (Exemplos: consultores e prestadores de serviços).

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

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

Integridade: capacidade de garantir que a informação esteja mantida em seu estado original, conforme foi concebida, a fim de protegê-la contra alterações indevidas, intencionais ou acidentais na guarda ou transmissão.

Informação: todo e qualquer conteúdo ou dado que tenha valor para alguma organização ou pessoa. Ela pode estar guardada para o uso restrito ou exposta ao público para consulta ou aquisição

Cyberbullying: prática negativa de assédio moral que afeta o psicológico de outra pessoa por meio de recursos tecnológicos, como publicações na internet e o envio de fotos e vídeos com mensagens ofensivas pelo celular ou qualquer outro dispositivo móvel.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável, como por exemplo: nome, sobrenome, e-mail, telefone, dados bancários, dados sobre salários.

Dado pessoal sensível: categoria especial de dados pessoais referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, referentes à saúde ou à vida sexual, dados genéticos ou biométricos relativos à pessoa natural.

Segurança da Informação: preservação da confidencialidade, integridade e disponibilidade da informação.

Vírus: programa malicioso que se propaga e infecta o computador.

Worm: programa semelhante ao vírus, que infecta o sistema, tendo como característica a auto replicação.

PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO NO CIETEC

Os equipamentos de informática, de comunicação, os sistemas e as informações devem ser utilizados para a realização de atividades profissionais, com senso de responsabilidade e preceitos éticos comuns à sociedade e dentro da legalidade.

Os colaboradores também devem usá-los para a realização de trabalho realizado internamente da organização.

É necessário respeitar a privacidade dos usuários, agindo de forma ética e atendendo aos princípios da Lei Geral de Proteção de Dados Pessoais. As senhas de acesso aos ambientes virtuais precisam ser seguras e não compartilhadas com terceiros.

O CIETEC reserva-se o direito de monitorar e registrar todo e qualquer uso das informações geradas, armazenadas ou veiculadas na organização. Assim, o uso dos equipamentos eletrônicos disponibilizados pelo CIETEC precisam ser utilizados apenas para o uso do trabalho.

RESPONSABILIZAÇÃO PELO MAU USO DOS EQUIPAMENTOS E PELO NÃO CUMPRIMENTO DESTA POLÍTICA

A responsabilidade em relação à Segurança da Informação deve ser atribuída na fase de contratação, de forma a ser incluída nos contratos e monitorada durante a sua vigência. Além de estender para os colaboradores, prestadores de serviços e terceiros, contratados em período anterior à publicação desta política, e que não tenham assinado os

respectivos documentos, deverá ser entregue um Termo de Ciência e Responsabilidade da PSI para a respectiva assinatura eletrônica.

Equipamentos adquiridos através de convênios, acordo, termos de fomento serão patrimoniados pela Secretaria e estarão sob a responsabilidade do CIETEC. Após o encerramento do convênio, acordo ou termo tais bens móveis serão incorporados ao patrimônio do Estado.

Todos os colaboradores, prestadores de serviços e terceiros que tenham acesso a informações do CIETEC, devem passar por treinamento e conscientização sobre os procedimentos de segurança e o uso correto dos ativos oferecidos pela organização.

A finalidade é minimizar possíveis riscos de segurança, explicitar as responsabilidades e comunicar os procedimentos para a notificação de incidentes. Todos os requisitos de Segurança da Informação e os aspectos legais, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de um projeto ou sistema. Também devem ser justificados, acordados, documentados, implementados e testados durante a fase de execução.

Assim, o mau uso das senhas, dos equipamentos eletrônicos, do compartilhamento de dados internos e qualquer outra prática em não conformidade com a segurança da informação gera responsabilidades para os colaboradores, prestadores de serviços e terceiros que trabalham, mesmo que por certo período no CIETEC.

É fundamental a compreensão e também a observância das políticas e diretrizes estabelecidas para proteger os dados contra acessos não autorizados, perdas ou violações de segurança. Além disso, é essencial que todos estejam cientes dos riscos associados ao manuseio inadequado dos dados e do impacto que uma violação de dados pode ter na reputação da imagem e o risco financeiro envolvido para o CIETEC.

BOAS PRÁTICAS

Ao seguir estas diretrizes e manter um compromisso contínuo com a proteção dos dados pessoais, o CIETEC demonstra seu comprometimento com a privacidade e segurança das informações de seus clientes e colaboradores, prestadores de serviços, fornecedores e terceiros vinculados direta ou indiretamente e que confiam as suas informações e dados pessoais ao CIETEC.

Colaboradores, prestadores de serviços e terceiros do CIETEC, em qualquer nível hierárquico, na sua esfera de competência, serão responsáveis por cumprir e zelar pela materialização e realização eficaz das normas e princípios da segurança da informação. Em atenção especial ao compromisso com os critérios legais e éticos que envolvem a organização.

É de inteira responsabilidade do usuário qualquer prejuízo ou dano sofrido ou causado ao CIETEC e/ou a terceiros, em decorrência da não obediência às diretrizes e às normas aqui referidas.

É também de responsabilidade do profissional o uso de senha segura, devendo alterá-la conforme periodicidade determinada pelo CIETEC.

Cabe a todos os usuários as seguintes práticas:

- Cumprir fielmente políticas, normas e procedimentos de Segurança da Informação, incluindo regras estabelecidas neste documento;
- Buscar orientação do superior quando houver dúvidas relacionadas à Segurança da Informação;
- Assinar o Termo de Responsabilidade, formalizando a ciência desta política e das normas de Segurança da Informação, bem como assumindo a responsabilidade pelo seu cumprimento;
- Considerar os usos de senha e acessos aos dispositivos corporativos: quem tem acesso, qual o acesso individualizado de cada um (por assinaturas digitais), controle de IP's etc.
- Manter todos os sistemas e dispositivos atualizados: as atualizações de software corrigem vulnerabilidades conhecidas, o que pode proteger sua organização contra ataques.

- Usar autenticação de duas fatores: a autenticação de duas fatores adiciona uma camada extra de segurança, exigindo que os usuários forneçam informações adicionais, além de uma senha, para acessar sistemas e dados.
- Criar backups regulares: Realizar backups regulares de seus dados é uma das formas mais eficazes de protegê-los contra perda ou destruição.
- Monitorar atividades de rede: mantenha um registro das atividades de rede para detectar atividades suspeitas ou mal-intencionadas.
- Usar *software* de segurança: instale software de segurança em todos os dispositivos e sistemas para protegê-los contra vírus, *spyware*, *malware* e outras ameaças.

TRABALHO REMOTO, HÍBRIDO E PRESENCIAL

Esta política de segurança da informação é direcionada também para todos que realizam trabalho remoto, híbrido e presencial.

Assim, todos devem zelar pelo bom uso do equipamento e também as senhas de acesso aos ambientes virtuais, além de ter cuidado nas reuniões online do dia a dia. Além disso, utilizar o email institucional de forma correta e com linguagem apropriada.

Pontos que precisam de cuidados:

- A segurança do ambiente físico, seja na modalidade de trabalho remoto ou presencial, é fundamental e contribui para a segurança das informações do dia a dia do trabalho; Pessoas que podem ter acesso aos dados, reuniões e informações são riscos que podem gerar um prejuízo nesta segurança.
- Os requisitos de segurança nas comunicações devem ser levados em consideração devido ao risco de vazamento de dados e informações ou mesmo o acesso aos sistemas internos da organização.

OCORRÊNCIA DE INCIDENTES DE SEGURANÇA E PLANO DE AÇÃO

Incidentes com dados pessoais referem-se a qualquer evento que possa resultar na violação da confidencialidade, integridade ou disponibilidade dos dados pessoais sob nossa responsabilidade, incluindo, mas não se limitando a:

- Acesso não autorizado ou divulgação de dados pessoais.
- Perda ou roubo de dispositivos que contenham dados pessoais.
- Ataques cibernéticos ou violações de segurança que comprometem os dados pessoais.
- Erros humanos que resultem na exposição inadequada de dados pessoais.

O Plano de Resposta estabelece as etapas a serem seguidas em caso de incidentes com dados pessoais, visando mitigar os impactos e proteger os direitos e interesses das partes afetadas. O plano deve incluir:

- Identificação e avaliação do incidente.
- Notificação imediata às autoridades competentes, se necessário.
- Isolamento e contenção do incidente para evitar danos adicionais.
- Investigação detalhada para determinar a extensão do incidente.
- Comunicação transparente e oportuna com as partes afetadas.
- Implementação de medidas corretivas para evitar futuros incidentes.

Ao ter ciência sobre qualquer incidente com dados pessoais, é preciso comunicar imediatamente o Setor de Compliance do CIETEC para que comunique o Encarregado de Dados e as providências iniciais para minimizar ou conter o incidente sejam tomadas com a maior brevidade possível, visando proteger os direitos dos titulares de dados e atuar em conformidade com o estipulado pela legislação.

RESPONSABILIDADE PELA GOVERNANÇA DOS DADOS E CULTURA DE CUIDADO



A responsabilidade com relação à governança e segurança dos dados é dever de todos os colaboradores e prestadores de serviço internamente e não somente do CIETEC, portanto, no exercício das suas funções, você deverá atentar-se e assumir o seu papel diante da responsabilidade coletiva em garantir a segurança, integridade e privacidade dos dados que manipulamos diariamente em decorrência das suas funções. Cada um desempenha um papel vital na governança de dados, independentemente da função ou nível hierárquico dentro do CIETEC.

É fundamental a compreensão e também a observância das políticas e diretrizes estabelecidas para proteger os dados contra acessos não autorizados, perdas ou violações de segurança. Além disso, é essencial que todos estejam cientes dos riscos associados ao manuseio inadequado dos dados e do impacto que uma violação de dados pode ter na reputação da imagem e o risco financeiro envolvido para o CIETEC.

Ao seguir estas diretrizes e manter um compromisso contínuo com a proteção dos dados pessoais, o CIETEC demonstra seu comprometimento com a privacidade e segurança das informações de seus clientes e colaboradores, prestadores de serviços, fornecedores e terceiros vinculados direta ou indiretamente e que confiam as suas informações e dados pessoais ao CIETEC.

DISPOSIÇÕES GERAIS

As infrações a esta política serão passíveis de processo disciplinar, podendo resultar a penalidades desde de mera advertência até demissão por justa causa e descontinuidade contratual do trabalho dos prestadores de serviço.

A qualquer tempo, e em qualquer um dos casos previstos, prevalecendo o descumprimento das regras expostas, o CIETEC poderá bloquear temporariamente o acesso do usuário e comunicar os motivos ao profissional e ao gestor da área.

O uso de qualquer recurso do CIETEC para atividades ilegais é motivo de demissão por justa causa e a instituição vai cooperar ativamente com as autoridades.

Diante das orientações desta política, a segurança deve ser entendida como parte fundamental da cultura interna do CIETEC.

DÚVIDAS

Em caso de dúvidas ou necessidade de esclarecimentos sobre esta Política, favor contatar seu superior hierárquico ou a área de Compliance.

REVISÃO

Esta Política será revisada a cada seis meses, ou em períodos menores, caso haja alguma circunstância específica que exija atenção especial e a área responsável pela atualização e revisão desta Política é a área de Compliance.

Última versão atualizada em julho de 2025.