CRA-TO
Conselho Regional de Administração do Tocantins

Conselho Regional de Administração de Tocantins

Fiscalizar, valorizar e promover o exercício do profissional de Administração, contribuindo com o desenvolvimento do país.

Gerência Executiva
Quadra 602 Norte Avenida Joaquim Teotônio Segurado Conjunto 01 Lote 06 - Bairro Plano Diretor Norte - Palmas-TO - CEP 77006-700
Telefone: (63) 3215-1240 - www.crato.org.br

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO Nº 1/2023/CRA-TO

PROCESSO Nº 476925.000497/2023-89

1. OBJETIVO

Definir diretrizes para utilização dos recursos computacionais (estações de trabalho, servidores, equipamentos de rede, internet, entre outros) visando à integridade dos recursos computacionais e sistemas informatizados, promovendo a segurança, preservação da confidencialidade, integridade e disponibilidade da informação, bem como, do acesso aos ambientes físicos do CRA – TO.

2. RESPONSABILIDADE

Setor de Tecnologia da Informação.

3. ABRANGÊNCIA

Colaboradores, prestadores de serviços e outras partes interessadas.

4. DOCUMENTOS COMPLEMENTARES

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação.

ABNT NBR ISO/IEC 27701:2019 – Tecnologia da Informação – Técnicas de segurança – gestão da privacidade da informação — Requisitos e diretrizes.

Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.

Lei de Acesso à Informação (LAI) 12.527 de 18/11/2011.

Lei de Direitos Autorais LEI Nº 9.610, de fevereiro de 1998

Lei Contra Software Pirata LEI 10.695 de 01/07/2003

Portaria CRA-TO nº 027/2023, de 26 de Maio de 2023 – Constituiu a Comissão de Privacidade e Proteção de Dados Pessoais.

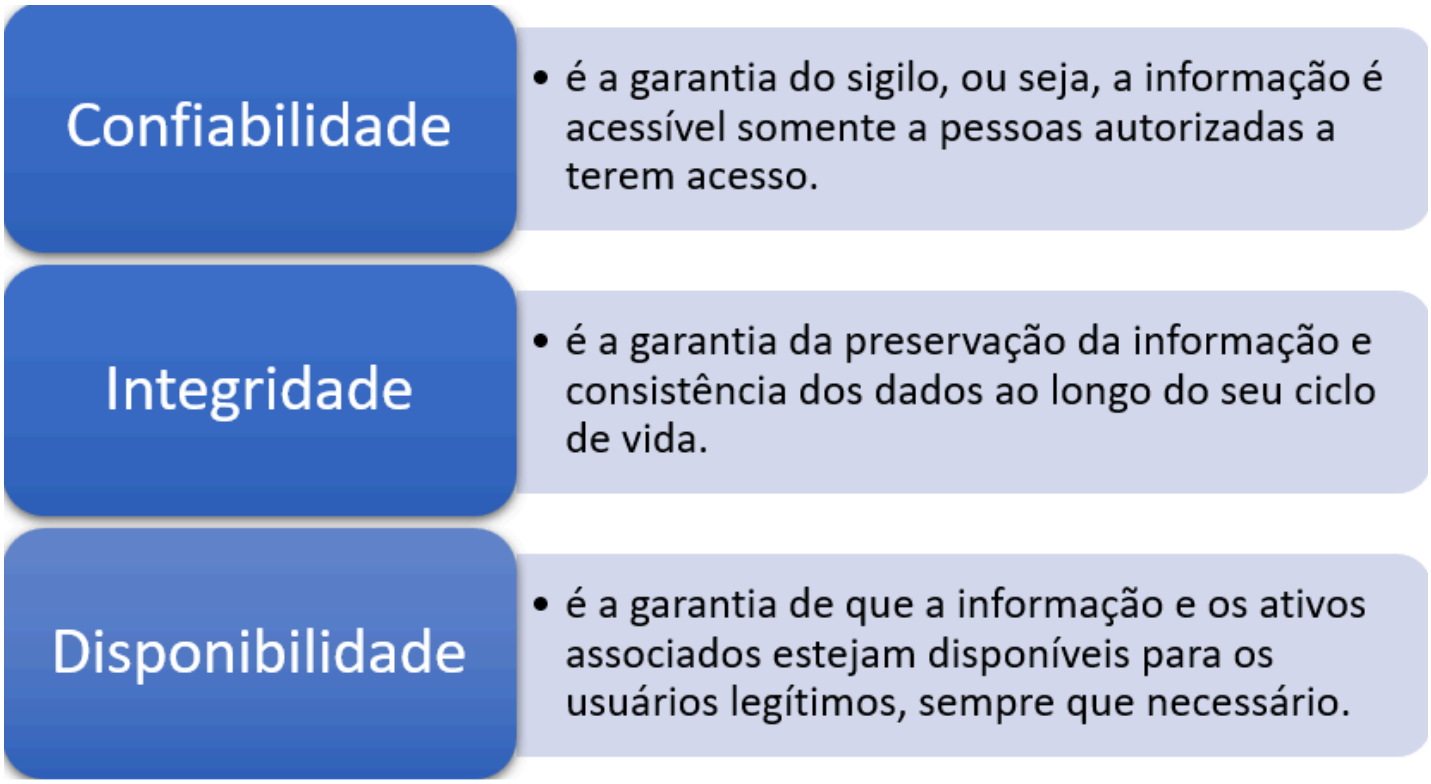
5. DESCRIÇÃO DO ESCOPO

5.1. Política de segurança da informação (PSI)

5.1.1. A informação é um ativo do Conselho Regional de Administração do Estado do Tocantins (CRA – TO), ou seja, é um bem que possui valor e, portanto, deve ser protegida, independentemente de ser escrita ou falada, impressa em papel, armazenada eletronicamente, transmitida pelo correio ou por outros meios eletrônicos.

5.2. A segurança da informação é alcançada através da preservação da confidencialidade, integridade e disponibilidade, assim entendidos:

Figura 1 – Pilares Segurança da Informação



5.1.3. A política da segurança da informação (PSI), trata da proteção aos ativos de informação nos aspectos físicos, tecnológicos e humanos, estabelecendo direitos e deveres para todos os atores envolvidos;

5.1.4. Estabelece diretrizes para a disponibilização e utilização de recursos de TI, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional, evitando expor qualquer informação que possa prejudicar o CRA – TO, seus funcionários, clientes ou parceiros;

5.1.5. Trata da gestão de continuidade das ações do CRA – TO frente a incidentes de segurança relativos aos ativos de informação;

5.1.6. Designa, define ou altera papéis e responsabilidades do grupo responsável pela Segurança da Informação;

5.1.7. Apoia a implantação das iniciativas relativas à Segurança da Informação;

5.1.8. Possibilita a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

5.1.9 Em conformidade com a legislação vigente, em especial com a Lei Federal nº 13.709/18 – Lei Geral de Proteção de Dados Pessoais (LGPD), o tratamento de dados pessoais deve observar os seguintes fundamentos:

I - Respeito à privacidade;

I - Autodeterminação informativa;

I - Liberdade e expressão;

I - Inviolabilidade da intimidade, honra e imagem;

I - Desenvolvimento econômico, tecnológico e inovação;

I - Livre iniciativa, livre concorrência e defesa do consumidor;

I - Diretos humanos, livre desenvolvimento da personalidade, dignidade e exercício da cidadania.

5.1.10. As ações referentes a tratamento de dados pessoais pelas entidades do CRA – TO devem atentar para a finalidade e necessidade do tratamento, a adequação dos processos e tecnologias, a qualidade dos dados coletados, assegurando tratamento isonômico, livre acesso aos dados por seu titular, transparência nas ações e segurança das informações.

5.2. Princípios da PSI

I - Toda informação produzida ou recebida pelos colaboradores, como resultado da atividade profissional, na qual o mesmo foi contratado pelo CRA – TO, pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes;

I - Os equipamentos de TI e sistemas de informações, deverão ser utilizados pelos colaboradores para realização das atividades inerentes à sua função.

I - O CRA – TO por meio de seu Setor de Tecnologia da Informação, poderá monitorar a utilização ou acesso aos recursos de TI no ambiente institucional, visando garantir a segurança da informação;

I - O CRA – TO preserva e protege as informações sob sua responsabilidade, dos diversos tipos de ameaça e desvios de finalidade em todo o seu ciclo de vida, estejam elas em qualquer suporte ou formato;

I - Previne e tratar impactos gerados por incidentes, envolvendo a segurança da informação.

I - As ações referentes ao tratamento de dados pessoais pelo CRA – TO deve atentar para a finalidade e necessidade do tratamento, a adequação dos processos e tecnologias, a qualidade dos dados coletados, assegurando tratamento isonômico, livre acesso aos dados por seu titular, transparência nas ações e segurança das informações;

I - Prevê recursos orçamentários com vistas a prover soluções e recursos, afim de mitigar impactos que possam gerar incidentes envolvendo a segurança da informação;

I - Assegura a confidencialidade, a integridade, a disponibilidade e a autenticidade, assim como a legalidade no desenvolvimento das atividades do negócio;

I - Cumpri a legislação vigente no Brasil e demais instrumentos regulamentares relacionados às atividades da Instituição no que diz respeito à segurança da informação, aos objetivos institucionais e aos princípios de privacidade, morais e éticos.

5.3. Das Definições

I - Para compreensão deste documento adotam-se os seguintes termos e definições:

I - PSI: Refere-se à Política de Segurança da Informação;

I - Ativos: todas as formas de criação, processamento, armazenamento, transmissão e exclusão de informações. Os ativos podem ser documentos impressos, sistemas, softwares, banco de dados, arquivos digitais, dispositivos móveis, etc.

I - Conta E-mail: Caixa postal para recebimento, armazenamento e envio de mensagens pelos usuários.

I - Confidencialidade: Garantia que o acesso à informação seja obtido somente por pessoas autorizadas.

I - Correio Eletrônico: Serviço de troca de mensagens eletrônicas através da rede de dados.

I - Conta de Rede: Autorização de utilização de serviços e acesso/armazenamento de informações nos Servidores.

I - Datacenter: é um local onde estão concentrados os sistemas computacionais de uma empresa ou organização, como um sistema de telecomunicações ou um sistema de armazenamento de dados;

I - Disponibilidade: Garantia de que usuários autorizados obtenham acesso a informações e aos ativos correspondentes sempre que necessário.

I - Login: Identificação única e exclusiva de um usuário que o identifica na rede utilizado para acessar os serviços da rede de dados.

I - Logon (autenticação): Processo de validação de acesso à rede de dados. No logon o usuário fornece o login e a senha para ser autenticado.

I - Log off: Processo de encerramento de acesso à rede de dados.

I - Incidente de segurança da informação com dados pessoais “vazamento de dados”: Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

I - Incidente de segurança da informação - É um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade ou confidencialidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação e Comunicações.

I - Incidente: Um incidente é qualquer evento que não faz parte da operação padrão de um serviço e que causa, ou pode causar, uma interrupção do serviço ou uma redução da sua qualidade.

I - Informação: Conjunto de dados, imagens, textos e quaisquer outras formas de representação, dotadas de significado dentro de um contexto.

I - Informação sensível ou crítica: Toda e qualquer informação cujo comprometimento possa causar perda de vantagem competitiva, dano ou prejuízo ao negócio ou à imagem da organização.

I - Integridade: Garantia de que as informações correspondem à sua descrição de forma única, exata, completa, de acordo com o método de processamento utilizado para sua obtenção.

I - Pasta: Local para armazenamento de arquivos dentro da rede de dados.

I - Segurança da Informação (SI): A informação é um ativo das organizações, ou seja, é um bem que possui valor e, portanto, deve ser protegida, independentemente de ser escrita ou impressa em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. A segurança da informação é alcançada através da preservação de três princípios: Confidencialidade, Integridade e Disponibilidade da informação (CID).

I - Senha: Conjunto de caracteres alfanuméricos que validam o usuário juntamente com seu login de acesso aos recursos da rede. A Senha é de caráter pessoal e intransferível e em momento algum deve ser compartilhada ou fornecida a terceiros.

I - Vulnerabilidade: Fragilidade de um ativo que pode ser explorada e gerar danos à organização.

I - Rede Administrativa do CRA: Rede Interna de computadores/servidores, instalados no âmbito administrativo na sede, dotada de política de segurança.

I - Recursos de Informática: Equipamentos e sistemas de informática pertencentes ao CRA - TO, empresas coligadas e clientes, tais como computadores, notebooks, servidores, impressoras, programas utilitários, arquivos, sistemas, aplicativos, internet e correio eletrônico

I - Mídias removíveis: são dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Pen Drive, cartão de memória, HDs portáteis, telefones celulares, entre outros que se utilizem de conexão USB.

I - Malwares: é qualquer software intencionalmente feito para causar danos a um computador, servidor, cliente, ou a uma rede de computadores;

I - VPN: VPN ou Virtual Private Network (Rede Privada Virtual) trata-se de uma rede privada construída sobre a infraestrutura da Internet.

I - Usuário: Todos os colaboradores e prestadores de serviços que utilizam os recursos de informática para realização de suas atividades diárias ou eventuais.

I - Pentest: Pentest ou teste de Intrusão, é um método capaz de avaliar a segurança de um sistema computacional ou de uma rede, simulando um ataque.

I - TIC: Tecnologia da Informação e Telecomunicação.

5.4. Diretrizes Gerais da Segurança da Informação

5.4.1. Interpretação e Divulgação da PSI

5.4.1.1. A presente Política e seus documentos complementares devem ser interpretados de forma restritiva, dentro do princípio de aplicação do menor privilégio possível, ou seja, no contexto de uso de informações e recursos de TI, tudo o que não estiver expressamente permitido só deve ser realizado após prévia validação da Comissão de Privacidade e Proteção de Dados Pessoais do CRA - TO e posterior autorização da Presidência, devendo ser levada em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

5.4.1.2.. A PSI deve ser divulgada para a Presidência, conselheiros, Gerência Executiva e demais colaboradores por meio da intranet e realização de capacitações, visando a disponibilização a todos os que se relacionam com o CRA - TO, de forma direta e indireta.

5.4.2. Classificação da Informação

5.4.2.1. Todas as informações de propriedade ou sob a responsabilidade do CRA - TO devem ser classificadas e protegidas com controles compatíveis em todo o seu ciclo de vida, por meio da implementação de ferramentas e formalização de processos em instrumento específico.

5.4.3. Conformidade

5.4.3.1. O CRA - TO deve possuir e manter um programa de revisão/atualização desta PSI e de seus documentos complementares. Anualmente deverá ser analisada a necessidade de revisão da PSI, ou quando mudanças significativas são propostas ou ocorrem, visando a garantia de que todos os requisitos de segurança técnicos e legais implementados sejam cumpridos, atualizados e em conformidade com a legislação vigente.

5.4.4. Privacidade e Proteção de Dados

5.4.4.1. O CRA - TO respeita a privacidade dos titulares de dados e garante a disponibilidade, integridade e confidencialidade dos dados pessoais em todo o seu ciclo de vida, que vai desde a coleta, armazenamento, compartilhamento, até o descarte, em qualquer tipo de formato de armazenamento e suporte de acordo com a sensibilidade do dado pessoal, a finalidade e a gravidade dos riscos, seguindo a Política de Privacidade de Dados e Proteção de Dados Pessoais e demais normativos e legislação aplicável.

5.4.5. Avaliação de Riscos

5.4.5.1. Os riscos identificados são avaliados e administrados em conformidade com os requisitos especificados em política própria para essa finalidade, bem como nos controles de proteção e as respostas, proporcionais aos riscos identificados.

5.5. Diretrizes para Uso dos Recursos de Tecnologia da Informação (TI)

5.5.1. Os recursos de TI de propriedade do CRA - TO devem ser utilizados apenas para fins profissionais, de modo lícito, ético, moral e aprovado administrativamente.

5.5.2. Os dirigentes, colaboradores e terceiros devem utilizar apenas recursos de TI previamente homologados e autorizados pelo Setor de Tecnologia da Informação (TI) para a realização de suas atividades profissionais, sejam eles onerosos, gratuitos, livres ou licenciados.

5.5.3. Não serão permitidos o uso de recursos de TI de propriedade particular, bem como, conexão dos mesmos, à rede administrativa do CRA - TO, para fins de execução de qualquer atividade no âmbito institucional.

5.5.4. Uso das Estações e Postos de Trabalho

5.5.4.1. Cada estação de trabalho (Desktop e Notebooks) configurado na rede administrativa do CRA – TO possui um nome único que permiti identifica–lo.

5.5.4.2. As estações de trabalho configuradas na rede administrativa do CRA - TO, possuem criptografia de dados habilitada a nível de pastas e arquivos, a fim de proteger as informações armazenadas nos diretórios pertencentes a conta de usuário.

5.5.4.3. O acesso às estações de trabalho, somente será possível por meio de autenticação, com as credenciais, de uso individual compostos de usuário e senha.

5.5.4.4. Não e permitido a instalação de software ou aplicações, por colaboradores, ou prestadores de serviço nas estações de trabalho. Este procedimento e restrito e autorizado apenas ao (s) colaborador (es) do Setor de TI.

5.5.4.5. As estações de trabalho conectadas à rede administrativa, possuem proteção através de antivírus, homologado, instalado e gerenciado pelo Setor de TI.

5.5.4.6. Não é permitido armazenar ou instalar nas estações de trabalho; softwares, arquivos de áudio, filmes, fotos pessoais ou informações que não sejam relacionadas às atividades institucionais, ou que não se enquadrem na Lei de Direitos Autorais.

5.5.4.7. Não e permitido a cópia de qualquer informação institucional, em mídia externa que não seja para uso exclusivo do CRA - TO, e não esteja devidamente autorizado pelo Gestor imediato.

5.5.4.8. Em hipótese alguma o CRA – TO se responsabilizará pela perda, corrupção ou uso indevido de informações e/ou dados particulares do usuário, eventualmente armazenados na sua estação de trabalho.

5.5.4.9. Ao se ausentar da sua estação de trabalho, o colaborador deve bloquear a sua sessão no computador, de forma a proteger o acesso aos sistemas ou informações ali armazenadas;

5.5.4.10. A instalação e desinstalação de qualquer equipamento de TI, para fins de movimentação, só poderá ser realizado com o acompanhamento técnico do Setor de TI.

5.5.5. Utilização da Rede Administrativa

5.5.5.1. Não é permitido a tentativa de acesso não autorizado, afim de fraudar a autenticação de usuário, para obtenção de acesso indevido em sistemas, ou colocar à prova a segurança da rede ou segurança de qualquer servidor. Isso inclui acesso aos dados não disponíveis, tais como; conexão a servidores, ou contas de usuários, cujo acesso não seja expressamente autorizado ao colaborador.

5.5.5.2. Não é permitida a utilização da rede, com intuito de comprometer a sua segurança, incluindo tentativas de provocar congestionamento, sobrecarga em servidores, bem como invasões.

5.5.5..3 Materiais de natureza pornográfica e racista não podem ser acessados, expostos, armazenados, distribuídos, editados ou gravados nos recursos computacionais da rede;

5.5.5.4. Jogos ou qualquer tipo de software/aplicativo não podem ser acessados, gravados ou instalados no diretório pessoal do usuário, no computador local ou em qualquer outro diretório da rede;

5.5.5..5. Não é permitido conectar à rede, equipamentos pessoais ou de terceiros.

5.5.5..6. Não são permitidas alterações das configurações de rede e/ou das máquinas, bem como, demais modificações que não sejam efetuadas pelo Setor de TI;

5.5.5.7. Quanto à utilização de equipamentos não institucionais, a exemplo de computadores, impressoras, entre outros, o CRA - TO não fornecerá acessórios, software ou suporte técnico, incluindo assistência para recuperar perda de dados.

5.5.5.8. O Setor de TI é o único autorizado a realizar e acompanhar Pentestes de segurança na rede administrativa, bem como em sistemas pertencentes ao CRA - TO, afim de identificar possíveis vulnerabilidades.

5.5.6. Uso e Armazenamento Pastas Compartilhadas em Rede

5.5.6.1. Os servidores de arquivos disponibilizados na sede do CRA - TO, permitem aos colaboradores, armazenar arquivos de forma segura, mantendo o uso comum centralizado, e compartilhado com acesso restrito para os colaboradores pertencentes ao seu respectivo setor.

5.5.6.2. Os arquivos serão armazenados em diretórios (Pastas Compartilhadas), conforme as permissões de acesso (leitura e/ou gravação) estabelecidas para o perfil de acesso do colaborador.

5.5.6.3 A gestão e governança dos servidores de arquivos do CRA – TO é de responsabilidade do Setor de TI, a qual define as diretrizes quanto a utilização deste recurso em âmbito institucional.

5.5.6.4. Cada setor possui uma cota de armazenamento fixa, disponibilizada no servidor de arquivos. Esta cota padrão é definida pelo Setor de TI com base na capacidade, a fim de garantir a disponibilidade do recurso;

5.5.6.5. Não é permitido habilitar o compartilhamento de diretórios e pastas nas estações de trabalho, conectadas à rede administrativa do CRA - TO, para armazenar ou compartilhar arquivos.

5.5.6.6. Não é permitido a utilização do servidor de arquivos para armazenamento de fotos, vídeos, músicas ou outros dados de caráter particular.

5.5.6.7. O compartilhamento de arquivos e informações entre as unidades ou departamentos internos, deve ser realizado por meio ferramentas tais como: OneDrive, biblioteca compartilhada, Grupo de Trabalho ou ferramenta de e-mail disponibilizadas na Plataforma em nuvem do office365, solução adotada pelo CRA - TO.

5.5.6.8. Não é permitido, o armazenamento de conteúdo institucional, tais como; fotos, áudio, vídeos, nos servidores de arquivos. Os mesmos deverão ser armazenados na plataforma de nuvem do office365, através das ferramentas OneDrive, biblioteca compartilhada ou Grupo de trabalho.

5.5.6.9. Não será permitido salvar na pasta compartilhada do servidor, arquivos do tipo executáveis ou compactados, ou qualquer conteúdo que possa oferecer algum risco a segurança.

5.5.6.10. Todos os arquivos armazenados nas pastas compartilhadas do servidor de arquivos que não estiverem em conformidade com a política de segurança da informação, serão excluídos de forma definitiva sem prévio aviso.

5.5.7. Uso e Armazenamento em Nuvem

5.5.7.1. A Plataforma Office365 é a solução homologada pelo Setor de TI do CRA - TO, e disponibilizada para armazenamento e compartilhamento em nuvem, onde dispõe de recursos a serem utilizados institucionalmente tais como: OneDrive, biblioteca compartilhada, grupo de trabalho, entre outros, cujo os acessos são administrados pelo Setor de TI.

5.5.7.2. Qualquer outra plataforma ou software de armazenamento e compartilhamento em nuvem, poderá ser bloqueada na rede administrativa do CRA - TO sem prévio aviso, e caso seja necessário a utilização, o mesmo poderá ser autorizado mediante a solicitação do gestor imediato, justificando a necessidade, através da abertura de chamado para o Setor de TI, que fara a análise e validação desta solicitação de acesso.

5.5.7.3. Ao término do contrato de trabalho do colaborador, todos os seus acessos aos recursos em nuvem serão revogados, sendo necessário que o gestor imediato solicite o backup dos dados no mesmo dia do seu desligamento. Após este prazo será realizado a exclusão da conta do usuário e o conteúdo armazenado no OneDrive ou no e-mail será perdido.

5.5.8. Uso de Softwares de Mensagens Instantâneas e Web Conferência

5.5.8.1. O Microsoft Teams, disponível na plataforma Office365 é a ferramenta homologada pelo CRA - TO, e disponibilizada para mensageria eletrônica e Web Conferência.

5.5.8.2. Não será permitido aos colaboradores, a utilização de outras ferramentas para mensageria eletrônica, com a finalidade de troca de informações institucionais ou para realização de web conferências internas ou externas.

5.5.8.3. Qualquer outra ferramenta que não seja homologada pelo Setor de TI, poderá ser bloqueada na rede do CRA - TO.

5.5.8.4. A utilização de outras ferramentas não homologadas, só poderão ser utilizadas, nos seguintes casos:

5.5.8.5. Em caso de reuniões pontuais, quando o demandante da reunião for terceiros, ou fornecedores, neste caso, o mesmo deverá encaminhar o link de acesso temporário da plataforma ou software de reunião que será utilizado;

5.5.8.6. Ou quando for devidamente autorizado pelo gestor imediato, e neste caso, o mesmo deverá justificar a necessidade mediante a abertura de chamado prévio ao Setor de TI, que procederá com análise e posterior atendimento, com base na justificativa apresentada.

5.5.8. Uso Correio Eletrônico

5.5.9.1. Todas as mensagens geradas ou transmitidas através do sistema de correio eletrônico são consideradas propriedade do CRA - TO, podendo ser monitoradas sem aviso prévio ou aprovação do usuário.

5.5.9.2. É proibido falsear, obscurecer, suprimir ou substituir a identidade de um usuário no sistema de correio eletrônico.

5.5.9.3. É proibido utilizar termos obscenos ou observações pejorativas em mensagens de correio eletrônico, bem como a circulação de:

I - Arquivos contendo vírus, jogos, áudio, vídeo, pornografia, pedofilia ou imagens que não estão relacionadas aos objetivos da CRA - TO;

II - Mensagens de propaganda ou venda de produtos com fins particulares;

I - Mensagens de correntes ou SPAM;

II - Mensagens de cunho religioso, racial, orientação sexual e política ou mencionando qualquer atividade ilegal;

III - Mensagens que forem de ajuda a colaboradores ou parentes devem ser comunicadas ao RH e distribuídas através de contas do Administrador de Correio ou de Comunicação Interna.

5.5.9.4. É recomendado que:

I - A desativação da auto execução de arquivos anexados a mensagens;

II - Desconfiar sempre dos arquivos anexados às mensagens, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido forjado e o arquivo anexado pode ser um vírus ou um cavalo de troia, programa que além de executar funções para as quais foi projetado, executa também outras funções, normalmente maliciosas e sem o conhecimento do usuário;

III - Não responder mensagens suspeitas de ser um SPAM, (e-mails não solicitados, que geralmente são enviados para um grande número de pessoas) e não enviar uma mensagem solicitando a remoção da lista, pois este é um dos métodos que os “spammers” utilizam para confirmar que o endereço do e-mail é válido.

5.5.10. Uso e Acesso à Internet

5.5.10.1. O acesso à Internet será autorizado para os colaboradores que necessitarem da mesma para o desempenho das suas atividades profissionais no âmbito institucional.

5.5.10.2. Todos os acessos à internet, provenientes da rede administrativa do CRA - TO serão passiveis de monitoramento e auditoria pelo Setor de TI, para fins de apuração de qualquer irregularidade no uso do recurso, que possa comprometer a segurança da rede.

5.5.10.3. A infraestrutura tecnológica, e serviços fornecidos para o acesso à internet são disponibilizados pelo CRA - TO, cabendo a TI, a gestão e análise do uso adequado do recurso. Caso necessário a mesma poderá bloquear qualquer aplicação, arquivo, site, correio eletrônico, domínio, ou aplicação armazenadas na rede/internet, visando assegurar o cumprimento desta PSI ou para garantir a conformidade com segurança da informação.

5.5.10..4. A utilização da internet para visitantes e prestadores de serviço será disponibilizada por meio de rede isolada e segmentada, através de conexão sem fio, devendo o responsável pelo setor demandante solicitar o acesso, previamente através da abertura de chamado à TI.

5.5.10.5. E proibido a utilização do serviço de Internet do CRA - TO, para realização de download/Uploud de software (Programas e Aplicativos) ou arquivos de (Vídeo e Áudio), ou conteúdo considerado delituoso, que não estejam em conformidade com a legislação nacional.

5.5.10.6. A utilização do acesso à Internet na rede administrativa, pelos colaboradores do CRA - TO é limitada às finalidades e necessidades da instituição e é vedado o uso para fins pessoais, sendo expressamente proibido acesso a sites constantes nas categorias informadas abaixo, sendo os mesmos bloqueados pelos sistemas de segurança da instituição, ou ainda que possam implicar em ações criminais ou possam comprometer as atividades institucionais, tais como sites com conteúdo relacionados à:

I - Violência, Ódio e Racismo

I - Nudismo, pornografia, Conteúdo Adulto

I - Armas, Drogas e Álcool

I - Jogos de azar

I - Hacking, proxy e P2P

I - Jogos

I - Humor e Piadas

I - Download de software e Malware

I - Filmes, Entretenimento

5.5.10.7. O acesso dos colaboradores, a conteúdo de redes sociais, tais como: (Instagram ou twitter) ou a conteúdo multimídia (youtube, vimeo) dentre outros, só será autorizado mediante a solicitação, através de abertura de chamado pelo responsável do setor demandante, justificando a necessidade do referido acesso.

5.5.10.8. Caso seja identificado algum bloqueio ou restrição de acesso à internet que não esteja infringindo a PSI, ou que esteja impactando diretamente às atividades institucionais, o colaborador deverá informar ao seu Gestor imediato, para que seja solicitada a liberação através da abertura de chamado à TI, com a devida justificativa.

5.5.10.9. Todas as solicitações de liberação de acessos à internet serão analisadas e avaliadas pela TI, e caso seja identificado algum impacto que possa comprometer as atividades institucionais ou a segurança da informação, o mesmo será submetido a Comissão de Privacidade e Proteção de Dados Pessoais, e a Presidência para deliberação.

5.5.1.1. Impressoras e Multifuncionais

5.5.11.1. O uso de equipamentos de impressão e reprografia devem ser feitos exclusivamente para impressão e/ou reprodução de documentos que sejam de interesse do CRA - TO ou que estejam relacionados ao desempenho das atividades profissionais do colaborador.

5.5.11.2. As impressões devem ser controladas através de usuário e senha individual ou por setor.

5.5.11.3. As cópias devem ser recolhidas na impressora sempre que forem impressas pelos usuários, principalmente quando se tratar de informações confidenciais e/ou sigilosas.

5.5.12.1. Utilização de Credenciais de Acesso

5.5.12.1. O usuário e senha de acesso à rede é único para cada colaborador e intransferível, pois assegura que apenas ele, devidamente identificado, utilize e mantenha os seus privilégios de acesso à informação.

5.5.12.2. O colaborador é responsável por todos os acessos e operações realizados através de sua senha, sendo expressamente proibida sua divulgação ou empréstimo, cabendo ao mesmo, a responsabilidade de manter o seu sigilo. Em caso de suspeita de perda de sigilo, o colaborador deve providenciar imediatamente a troca de sua senha.

5.5.12.3. Será concedida ao colaborador senha padrão de acesso, que deverá ser alterada imediatamente no primeiro acesso.

5.5.12.4. Com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras.

5.5.12.4.1. A definição de senha deve, por medida de segurança, obedecer à seguinte formação:

I - Uso de 6 (seis) ou mais caracteres;

I - Existência de no mínimo uma letra maiúscula, letras minúsculas, composta por dígitos numéricos e caracteres especiais;

I - O colaborador deve evitar senhas compostas de elementos facilmente identificáveis por possíveis invasores, como por exemplo: nome, sobrenomes, datas, placas de carros, números de documentos e telefones, entre outros.

I - Não é recomendado a utilização de sequenciais do teclado, ou seja, associadas à proximidade entre os caracteres no teclado do computador como por exemplo (ASDFG, YUIOP, Cvbn12345);

I - Nunca compartilhar quaisquer credenciais de acesso com outras pessoas. Essa recomendação é importante não apenas para as contas de usuários utilizadas nos sistemas e serviços no âmbito do CRA - TO, mas também para a utilização dos diversos serviços que fazem parte do dia a dia de cada pessoa como, e-mail, serviços bancários, entre outros.

I - As senhas de acesso devem ser alteradas a cada 90 dias;

I - Não serão permitidas senhas para grupos de usuários ou que um usuário tenha mais de duas credenciais de acesso à rede.

I - Após o cadastramento do usuário na rede, este receberá uma senha provisória que será informada por telefone ou e-mail, possibilitando sua ativação na rede.

I - Esta senha provisória deverá ser alterada no primeiro logon do usuário. Caso isto não ocorra, esta senha será revogada num prazo máximo de 5 (cinco) dias. A partir daí o usuário será obrigado a recomeçar o processo de cadastramento de senha.

5.5.12.4.2. As credenciais do colaborador poderão ser bloqueadas do acesso à rede e/ou aos sistemas de informação, nas seguintes situações:

I - Rescisão ou término contratual do colaborador com a instituição;

I - Mudança de função ou alteração de setor;

I - Após ter o acesso negado por consecutivas tentativas sem sucesso;

I - Em caso de suspeita de violação ou ameaças à segurança;

I - Por solicitação do Gestor imediato ou Presidência;

I - Ou por solicitação do colaborador, neste caso, desde que autorizado pelo seu Gestor.

5.5.12.4.3. Em caso de bloqueio da credencial de acesso, o desbloqueio poderá ser solicitado pelo usuário desde que autorizado.

5.5.6. Backup e Recuperação de Dados

5.5.6.1. Os arquivos armazenados nos servidores são protegidos contra perdas diversas por meio de backup periódicos. Os arquivos salvos no disco rígido das estações de trabalho não são protegidos e, portando sujeitos a perdas.

5.5.6.2. O usuário deverá armazenar seus arquivos na sua respectiva área no servidor. O CONSELHO REGIONAL DE ADMINISTRAÇÃO DO TOCANTINS não tem responsabilidade pela recuperação de arquivos salvos nas estações dos usuários.

5.5.6.3. Caso haja uma perda acidental de arquivo do usuário, uma recuperação do backup anterior poderá ser solicitada.

5.5.7. Controle de Acesso

5.5.7.1. Controle e Acesso aos Ambientes Físicos:

5.5.7.1.1. O colaborador deverá portar de forma bem visível sua credencial de acesso (crachá).

5.5.7.1.2. Visitantes e prestadores de serviços, devem ser identificados na recepção e receber uma etiqueta/crachá de identificação para ser utilizado em local visível.

5.5.7.1.3. O ingresso às áreas restritas e de segurança somente será permitido com acompanhamento de colaborador designado pela gerência executiva a ser visitada.

5.5.7.1.4. O acesso as dependências da TI, bem como as salas de Telecomunicações são ambientes restritos, apenas o Setor de Tecnologia da Informação ou pessoa devidamente autorizada.

5.5.7.1.5. Fora do horário de expediente, feriados e finais de semana o acesso as dependências do CRA – TO, somente será realizada com a devida autorização e com antecedência mínima, desde que devidamente justificada junto a Gerência Executiva, Presidência ou Diretoria Administrativa e Financeira.

5.6. Papéis e Responsabilidades

5.6.1. Da Comissão de Privacidade e Proteção de Dados Pessoais.

O Sistema de Gestão de Segurança da Informação possui apoio consultivo do Comitê de Privacidade e Proteção de Dados Pessoais do CRA – TO.

5.6.2. Da Presidência, Diretoria, Conselheiros, Colaboradores, Clientes, Parceiros e Terceiros:

I - Cumprir as determinações desta Política de Segurança da Informação, bem como os respectivos documentos complementares;

I - Proteger a informação contra acesso não autorizado, divulgação, modificação, destruição ou interferência, em todo seu ciclo de vida;

I - O cumprimento desta Política faz parte das responsabilidades de trabalho e, a partir de sua publicação deve integrar os contratos de trabalho e contratos com fornecedores em que suas disposições forem aplicáveis.

5.6.3. Do Setor de Tecnologia da Informação:

I - Fornecer o embasamento técnico necessário ao responsável pelo tratamento de dados pessoais ou a Comissão de Privacidade e Proteção de Dados Pessoais, para subsidiar as informações solicitadas;

I - Coordenar a implantação dos controles e processos de segurança da informação aprovados pela Presidência;

I - Identificar fragilidades e ameaças significativas às informações e propor as tratativas cabíveis;

I - Realizar periodicamente análise crítica independente para verificação da eficácia do Sistema de segurança da informação.

5.7. DISPOSIÇÕES FINAIS

5.7.1. Este documento, dentre outras diretrizes, dá ciência aos envolvidos, de que os ambientes, sistemas, recursos computacionais e redes informacionais poderão ser monitorados, com prévia informação, conforme previsto na legislação brasileira.

5.7.2. Segurança da Informação é um fator crítico para a continuidade do negócio. O sucesso desta Política de Segurança da Informação está intimamente relacionado ao compromisso de todos no CRA - TO em realizar suas atividades do cotidiano conforme as diretrizes estabelecidas.

5.7.3. Os casos não previstos nesta Política de Segurança da Informação serão submetidos à análise da Comissão de Privacidade e Proteção de Dados Pessoais do CRA - TO e posterior autorização da Presidência.

5.7.4. O descumprimento desta Política de Segurança da Informação estará sujeito às medidas disciplinares.

6. REGISTROS

Não se aplica.

7. ANEXOS

Não se aplica

8. DOCUMENTOS RELACIONADOS

Não se aplica.

9. APROVAÇÃO

Anderson Justino Martins

Presidente do CRA - TO

Elaboração Conteúdo

João Marcus Ferreira Cavalcante (TI)

Adm. Aurivan de Castro (Encarregado de Dados)

Revisão

Dra. Isabella Sousa Feitosa (Assessoria Jurídica)

Admª. Laricy Aires Capistrano

Lana Milena Neiva Leite

Márcia Betânia Alves Pereira

Adm. Kleber Rodovalho de Souza

Hitler Pacheco Machado

Leirinalva Cruz Rodrigues

Raioneide Maria Nascimento da Silva

(assinado eletronicamente)
Adm. Anderson Luiz Justino Martins
Diretor Adm. Financeiro CRA-TO
CIP nº 00491

(assinado eletronicamente)
Adm. Aurivan de Castro
Presidente CRA-TO
CIP nº 00690

(assinado eletronicamente)
João Marcus Ferreira Cavalcante
TI CRA-TO

(assinado eletronicamente)
Dra. Isabella Sousa Feitosa
Assessoria Jurídica CRA-TO

(assinado eletronicamente)
Admª Laricy Aires Capistrano

Gerencia CRA-TO
CIP nº 02915

(assinado eletronicamente)
Adm. Kleber Rodovalho de Souza

Conselheiro CRA-TO
CIP nº 00690

(assinado eletronicamente)
Lana Milena Neiva Leite
Assistente Administrativo CRA-TO

(assinado eletronicamente)
Márcia Betânia Alves Pereira
Coordenadora Administrativa CRA-TO

(assinado eletronicamente)
Hitler Pacheco Machado
Assistente Administrativo CRA-TO

(assinado eletronicamente)
Leirinalva Cruz Rodrigues
Analista Administrativa CRA-TO

(assinado eletronicamente)
Raioneide Maria Nascimento da Silva
Assistente Administrativo

Documento assinado eletronicamente por **Adm. Aurivan de Castro**, **Diretor(a)**, em 19/10/2023, às 17:33, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **Laricy Aires Capistrano**, **Gerente Executivo(a)**, em 19/10/2023, às 17:44, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **Adm. Kleber Rodovalho de Souza**, **Conselheiro(a)**, em 19/10/2023, às 18:04, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **Adm. Anderson Luiz Justino Martins**, **Presidente**, em 19/10/2023, às 18:12, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **João Marcus Ferreira Cavalcante**, **Usuário Externo**, em 20/10/2023, às 06:30, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **Lana Milena Neiva Leite**, **Assistente Administrativo(a)**, em 20/10/2023, às 09:17, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **Hitler Pacheco Machado**, **Assistente Administrativo(a)**, em 20/10/2023, às 12:37, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **Leirinalva Cruz Rodrigues**, **Analista Administrativo(a)**, em 20/10/2023, às 12:44, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **Isabella Sousa Feitosa**, **Assessor(a) Jurídico(a)**, em 20/10/2023, às 14:37, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **Marcia Betania Alves Pereira**, **Coordenador(a) Administrativo(a)**, em 20/10/2023, às 14:38, conforme horário oficial de Brasília.

Documento assinado eletronicamente por **Raioneide Maria Nascimento da Silva**, **Assistente Administrativo(a)**, em 26/10/2023, às 12:19, conforme horário oficial de Brasília.

A autenticidade deste documento pode ser conferida no site sei.cfa.org.br/conferir, informando o código verificador **2240817** e o código CRC **0F2803D6**.

Referência: Processo nº 476925.000497/2023-89 SEI nº 2240817