SERVIÇO PÚBLICO FEDERAL

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO CEARÁ

CONSELHO SUPERIOR

RESOLUÇÃO N° 023, DE 27 DE MARÇO DE 2017

Aprova a Política de Segurança da Informação do IFCE.

O PRESIDENTE DO CONSELHO SUPERIOR DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO CEARÁ, no uso no uso de suas atribuições legais e estatutárias e considerando a deliberação do Conselho Superior na 43ª reunião ordinária realizada nesta data;

R E S O L V E:

Art. 1º - Aprovar a Política de Segurança da Informação do Instituto Federal de Educação, Ciência e Tecnologia do Ceará, conforme anexo.

Art. 2º - Esta Resolução entra em vigor a partir da data de sua publicação.

Virgílio Augusto Sales Araripe
Presidente do Conselho Superior

INSTITUTO FEDERAL
Ceará

TÍTULO I

DAS DISPOSIÇÕES GERAIS

CAPÍTULO I

DO OBJETIVO

Art. 1 º Esta Norma dispõe sobre as Diretrizes Básicas da Política de Segurança da Informação, a serem cumpridas no âmbito do Instituto Federal de Educação, Ciência e Tecnologia – IFCE, referentes ao conjunto de medidas de proteção, composto de normas e procedimentos que, quando aplicado aos ativos de informações, possa nortear o IFCE quanto à garantia aos Princípios de Segurança da Informação de confidencialidade, integridade, disponibilidade, autenticidade e confidencialidade.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 2º O Instituto atua em conformidade com os procedimentos estabelecidos nesta Norma, observando os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, da finalidade, do interesse público, da transparência e da motivação dos atos administrativos, exonerando-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

CAPÍTULO III

DO ESCOPO

Art. 3º As Diretrizes Básicas da Política de Segurança da Informação do IFCE referem-se a:

I - aos aspectos estratégicos, estruturais e organizacionais, preparando a base para elaboração dos documentos normativos que as incorporarão; e

II - aos requisitos de segurança humana, física e lógica que dão sustentação aos procedimentos, dos processos de trabalho e dos ativos de informação que influirão diretamente nos produtos e serviços ofertados pelo IFCE.

INSTITUTO FEDERAL
Ceará

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 4º As responsabilidades para a Gestão da Segurança da Informação são atribuídas da seguinte forma:

I – Comitê de Tecnologia da Informação: aprovar a Política de Segurança da Informação e suas revisões, designar os proprietários da informação se necessário, e tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelo Grupo de Trabalho de Segurança da Informação.

II – Grupo de Trabalho de Segurança da Informação - GTSI: órgão colegiado, nomeado pela Comitê de Tecnologia da Informação do IFCE, cuja composição, forma de deliberação e periodicidade de reuniões é normatizada em Portaria específica, sendo responsável: por analisar e propor medidas para efetiva aplicação, disseminação e aprimoramento da Política de Segurança da Informação; pelo acompanhamento e a alocação de recursos financeiros, humanos e tecnológicos, projetos e iniciativas de Segurança da Informação; pela definição sobre a existência de área específica para Gestão da Segurança da Informação, voltada para Gestão de Riscos; por dirimir dúvidas e a propriedade (“ownership”) dos ativos de informação;

III – Ouvidoria: responsável pela implementação e acompanhamento da Lei de Acesso à Informação Pública e pelo SIC – Serviço de Informações ao Cidadão;

IV – Diretoria de Gestão de Tecnologia da Informação – DGTI: regulamentar e operacionalizar os normativos provenientes da Política de Segurança da Informação, o que inclui manutenção do parque computacional (é vedada a abertura de computadores para qualquer tipo de reparo), implantação do Datacenter, bloqueio de sites e endereços, trilhas de auditoria, bloqueio e periodicidade da troca de senhas de usuários, Plano de Continuidade do Negócio, Política de Backup, Acordos de Nível de Serviço, inventário atualizado dos ativos de informação, proteção contra invasões e malware, homologação, instalação, remoção e atualização de softwares, adição ou retirada de dispositivos computacionais na rede do campus, configuração de qualquer tipo referentes a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro, e o monitoramento e pronta resolução de incidentes;

V – Pro-Reitoria de Gestão de Pessoas – PROGEP: executar as ações de Treinamento e Desenvolvimento referentes à Segurança da Informação, bem como colher a assinatura do Termo de Responsabilidade dos colaboradores, estagiários e terceirizados, arquivando-os nas pastas respectivas, informando ao GTSI os desligamentos e afastamentos do quadro funcional que porventura houver para remoção imediata das autorizações dadas;

INSTITUTO FEDERAL
Ceará

VI – Assessoria de Comunicação Social – ASCOM: executar as atividades relacionadas à comunicação institucional, divulgando e disseminando as orientações emanadas pela Política de Segurança da Informação;

VII – colaboradores: como custodiantes, devem observar e acatar as recomendações para a utilização segura dos recursos dos ativos de informação e, em caso de dúvidas ou problemas, tais como sites ou e-mails suspeitos, roubo ou extravio de informações ou equipamentos sob sua custódia, contatar prontamente a DGTI.

Art. 5º As determinações contidas nas regras e diretrizes são obrigatórias e necessárias.

TÍTULO II

DA CONCEITUAÇÃO

Art. 6º Para fins de uniformidade dos procedimentos contidos nesta Norma são adotados os conceitos a seguir:

I – acesso privilegiado: acesso que permite ao administrador de serviço sobrepor controles do sistema de informação e somente deve ser concedido àqueles que o necessitam para a condução de suas atividades;

II – administrador de serviços: colaborador que possui acesso privilegiado para a utilização e disponibilização, por força de suas funções, de recursos restritos de Tecnologia da Informação;

III – ativo: tudo que manipula a informação, inclusive ela própria, tais como processos administrativos, bases de dados e arquivos, documentação de sistema, manuais, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas, softwares, sistemas, ferramentas de desenvolvimento e utilitários, estações de trabalho, servidores, equipamentos de comunicação, no-breaks e outros;

IV – autenticidade: garantia de que o acesso, transmissão ou alteração de dado ou informação é feito através de canais verdadeiros e fidedignos tanto na origem como no destino;

V – Caráter ostensivo – grau de inexistência de sigilo de informação, sendo passível de acesso por qualquer cidadão;

VI – Caráter reservado – grau de sigilo de informação que indica o impedimento de acesso à mesma, por pessoa não autorizada, até o prazo máximo de 5 anos;

VII – colaborador: agente público em exercício no IFCE, podendo ser titular de cargo efetivo, contratado por tempo determinado ou prestador de serviço terceirizado;

INSTITUTO FEDERAL
Ceará

VIII – confidencialidade: garantia do acesso autorizado ao ativo de informação, de acordo com seu nível de proteção, cuja classificação será regulada em norma específica pelo IFCE;

IX – Custodiante da informação: qualquer pessoa que usa, guarda ou tramita ativo de informação, cuja origem ou destino não seja proprietário;

X – disponibilidade: garantia de que os colaboradores possam ter acesso a informações segundo sua demanda. Pode ser crítica, que exige recuperação imediata em caso de perda, ou normal, quando a recuperação pode se dar em espaço de tempo maior;

XI – integridade: garantia de que as informações e métodos de processamento somente sejam alterados mediante ações planejadas e autorizadas; o controle de alterações pode ser básica (sem log) ou controlada (trilha de auditoria);

XII - medidas de proteção: medidas destinadas a garantir o sigilo, quando necessário, a inviolabilidade, a integridade, a autenticidade, a legitimidade e a disponibilidade de dados e informações, com o objetivo de prevenir, detectar, anular ou registrar ameaças reais ou potenciais a dados e informações;

XIII - não-repúdio: garantia de que o emissor da mensagem não irá negar posteriormente a autoria da mensagem ou transação, permitindo a sua identificação;

XIV – plano de contingência/continuidade do negócio: plano que descreve as ações que uma organização deve tomar para assegurar a continuidade dos processos críticos em caso de sinistros na organização ou falhas nos sistemas, incluindo a ativação de processos manuais, duplicidade de recursos, traslado de pessoal e acionamento de fornecedores;

XV – política de segurança da informação: recomendações com o propósito de estabelecer critérios para o adequado manuseio, armazenamento, transporte e descarte das informações através do desenvolvimento de Diretrizes, Normas, Procedimentos e Instruções destinadas, respectivamente, aos níveis estratégico, tático e operacional;

XVI – princípios da segurança da informação: princípios da confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio, que regem a segurança da informação, de acordo com o art. 3° do Decreto n° 3.505, de 13 de junho de 2000;

XVII – Proprietário da Informação: trata-se do gestor designado de sua área organizacional que responderá pela concessão, manutenção, revisão, registro e cancelamento de autorizações de acesso a ativos de informação de sua área jurisdicionada quando se tratar de informação reservada;

XVIII – Sigilo: propriedade da informação que indica o impedimento de acesso à mesma por pessoa não autorizada; e

XIX – termo de responsabilidade: acordo de confidencialidade para não divulgação de informações, atribuindo responsabilidades ao colaborador e administrador de serviço

INSTITUTO FEDERAL
Ceará

quanto ao sigilo e a correta utilização dos ativos de propriedade ou custodiados pelo IFCE, cujo teor será explicitado por norma interna para uso de equipamentos de informática, de sistemas e da rede de comunicações do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA – IFCE.

TÍTULO III

DAS DIRETRIZES

CAPÍTULO I

DOS REQUISITOS

Art. 7º As Diretrizes Básicas da Política de Segurança da Informação devem atender às seguintes normas:

I - Lei 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso à informação pública;

II - Decreto nº 7.724, de 16 de maio de 2012 que regulamenta o acesso à informação pública;

III - a Lei nº 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

IV - o Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades de Administração Pública Federal;

V – Artigo 307 do Código Penal Brasileiro (Decreto Lei 2.848/40) que pune a falsa identidade;

VI – Seção 5 da norma ABNT NBR ISO/IEC 27002, código de prática que estabelecem diretrizes e princípios gerais para iniciar e manter a Gestão de Segurança da Informação; e

VII – a Instrução Normativa GSI/PR nº 01/2008 que disciplina a Gestão da Segurança da Informação e Comunicações no âmbito da Administração Pública Federal e suas normas complementares.

INSTITUTO FEDERAL
Ceará

CAPÍTULO II

DA CAPACITAÇÃO E APERFEIÇOAMENTO

Art. 8º As Diretrizes Básicas da Política de Segurança da Informação devem ser divulgadas na Unidade Organizacional, garantindo que todos tenham consciência da política e a pratiquem na organização.

Parágrafo único. Todos os colaboradores devem obedecer ao disposto nas Diretrizes Básicas da Política de Segurança da Informação, recebendo as informações necessárias para o seu adequado cumprimento.

Art. 9º Os colaboradores devem ser continuamente capacitados para o uso dos ativos de informação quando da realização de suas atividades.

Art. 10. Programas de conscientização sobre segurança da informação serão implementados através de treinamentos específicos, assegurando que todos os colaboradores sejam informados sobre os potenciais riscos de segurança e o tipo de exposição a que estão submetidos os sistemas de informações e operações do IFCE e suas partes interessadas.

Art. 11. Os treinamentos a serem disponibilizados devem estar compatíveis com as tecnologias atualmente implementadas no ambiente informatizado, e pelas demais que porventura venham a ser adotadas.

CAPÍTULO III

DO ACESSO, PROTEÇÃO E GUARDA DA INFORMAÇÃO

Art. 12. A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade.

Art. 13. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IFCE é considerada seu patrimônio e deve ser protegida conforme estabelecido nesta Norma.

Parágrafo único. Qualquer falha na segurança da informação, identificada por qualquer colaborador, deve ser imediatamente comunicada ao seu superior imediato, que a encaminhará ao GTSI para avaliação e determinação das ações que se fizerem necessárias.

Art. 14. É vedado o controle exclusivo, por apenas um colaborador, de um processo de negócio ou recurso.

Art. 15. Todos os colaboradores que manipulem ou tenham acesso a informações identificadas como reservadas sob custódia ou propriedade do IFCE, devem garantir a

INSTITUTO FEDERAL
Ceará

confidencialidade e o sigilo destas informações, adotando comportamento seguro, caracterizado por evitar assuntos reservados em ambientes sociais e particulares, a impressão, transmissão, compartilhamento e transporte para fora das instalações do IFCE, de informação reservada sem autorização, e o uso e não compartilhamento de senhas seguras;

Art. 16. As violações de segurança devem ser comunicadas e registradas, e esses registros, analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria.

CAPÍTULO IV

DA UTILIZAÇÃO DOS RECURSOS

Art. 17. Os recursos disponibilizados são fornecidos com o propósito único de garantir o desempenho das atividades do IFCE, sendo vedado aos colaboradores: o uso desses recursos para constranger, assediar, ofender, caluniar, ameaçar ou causar prejuízos a qualquer pessoa física ou jurídica; armazenar, transmitir ou compartilhar arquivos pessoais ou não relacionados às suas atividades nos recursos corporativos da rede interna, tais como vídeos, fotos, músicas, jogos, apresentações e apostilas; quaisquer outras atividades que contrariem os objetivos institucionais do IFCE.

Art. 18. Os acessos à rede de dados do IFCE são gerenciados em todos os tipos de conexão, devendo os colaboradores ser identificados e ter acessos apenas às informações e aos recursos tecnológicos necessários ao desempenho de suas atividades.

Art. 19. Todos os ativos de informação do parque computacional devem ser inventariados, incluindo-se dispositivos móveis como notebooks, handsets, tablets e smartphones, quando pertencentes ao IFCE, com identificação patrimonial e de seus responsáveis, bem como a definição de suas configurações, manutenções e documentações pertinentes, implementando-se senha de BIOS quando aplicável.

Parágrafo único. Todo o ativo de informação deve ser protegido e conservado, de forma a preservar os seus componentes internos, externos e acessórios.

CAPÍTULO V

DA COMUNICAÇÃO ELETRÔNICA

Art. 20. Toda informação veiculada eletronicamente será alvo de controle e monitoração, e seu uso deve ser tão somente para fins corporativos relacionados às atividades do colaborador dentro da instituição, sem posicionamento pessoal, político, sexual ou religioso, devendo seu comportamento ser decoroso e de acordo com a legislação em redes sociais e assemelhados, quando se identificar como colaborador do IFCE ou durante o horário de expediente, mantendo as informações de caráter reservado protegidas e comunicando prontamente ao GTSI quaisquer eventos de quebra de

INSTITUTO FEDERAL
Ceará

segurança, tais como recebimento de informação sigilosa por engano, ataques, adulteração e roubo de informação.

Parágrafo único. A Política de Segurança da Informação prevê mecanismos que visem a garantir e proteger a informação quanto à autenticação e ao uso responsável dos recursos computacionais do IFCE.

CAPÍTULO VI

DA SEGURANÇA FÍSICA E DO AMBIENTE E DE RECURSOS HUMANOS

Art. 21. Tendo em vista a necessidade de se garantir a segurança física e do ambiente, bem como a segurança de recursos humanos, o IFCE estabelecerá controles, visando a:

I - prevenir o acesso físico indevido e sem autorização, bem como danos e interferências com as instalações e informações do IFCE; e

II – assegurar que os colaboradores, fornecedores e terceiros entendam suas responsabilidades e assinem acordos sobre seus papéis e responsabilidades pela segurança da informação, com a finalidade de reduzir os riscos de burla, erros humanos, furto, roubo, apropriação indébita, fraude, ou uso indevido dos ativos de informações do IFCE.

CAPÍTULO VII

DO PLANO DE CONTINUIDADE

Art. 22. Os procedimentos que garantam a continuidade e a recuperação do fluxo de informações devem ser mantidos, observando-se as classificações de disponibilidades requeridas, de forma a não permitir a interrupção das atividades de negócios e proteger os processos críticos contra falhas e danos, que atenderão aos seguintes objetivos:

I - avaliação em regime emergencial das consequências de desastres, falhas de segurança e perda de serviços;

II - contingência e recuperação do funcionamento normal dentro de períodos de tempos determinados; e

III - recuperação tempestiva das operações consideradas vitais.

INSTITUTO FEDERAL
Ceará

CAPÍTULO VIII

DA CONFORMIDADE

Art. 23. Devem ser adotados procedimentos apropriados para garantir a conformidade e o respeito às restrições legais quanto ao uso e disseminação de informações protegidas por leis tais como: dados pessoais relativos à intimidade, à vida privada, à honra e à imagem, de propriedade intelectual, direitos autorais, segredos comerciais e de indústria, patentes e marcas registradas, ou aquelas classificadas como reservadas.

Art. 24. Os processos de aquisição de bens e serviços, especialmente dos ativos de informação, devem estar em conformidade com esta Norma.

Art. 25. Os sistemas de informações, além de disponibilizar os registros em prazos e formatos aceitáveis, devem protegê-los contra perda, destruição e falsificação, visando à salvaguarda dos dados.

CAPÍTULO IX

DA CLASSIFICAÇÃO E DO SIGILO DA INFORMAÇÃO

Art. 26. Toda informação não classificada terá caráter ostensivo, e deverá ser fornecida a qualquer cidadão identificado que a solicitar, em formato aberto, independente de motivação, exceto aquela que se inclua no disposto no Art. 23 desta norma.

Art. 27. Será passível de classificação qualquer informação que provoque riscos à vida, segurança ou saúde da população, ou riscos à defesa, economia ou relações internacionais do Estado, e aquela que, no âmbito do IFCE, provoque assimetria competitiva ou privilégio entre agentes regulados, exponha o IFCE a ataques ou fraudes, ou que pertença a normas, autorizações, estudos e fiscalizações que componham processo não concluído.

Art. 28. Informação classificada com disponibilidade crítica, se houver, deverá estar coberta pelo Plano de Continuidade do Negócio.

Art. 29. Toda informação classificada será considerada de integridade controlada.

Parágrafo único. A Política de Segurança da informação e os Sistemas de Informação do IFCE deverão garantir a executoriedade do sigilo resultante da classificação da informação, a ser regulamentada em norma específica, e também a disponibilidade, integridade, autenticidade e confidencialidade da Informação do IFCE, independentemente de sua classificação.

INSTITUTO FEDERAL
Ceará

TÍTULO IV

DAS DISPOSIÇÕES FINAIS

CAPÍTULO I

DA AVALIAÇÃO E DA REGULAMENTAÇÃO

Art. 30. O cumprimento desta Norma deve ser avaliado periodicamente, de acordo com os critérios do GTSI.

Art. 31. Fica a DGTI autorizada a regulamentar, e submeter à Reitoria do IFCE para aprovação, os procedimentos necessários para a aplicação das disposições estabelecidas nesta Norma que estarão consubstanciadas na norma interna que regulamenta o uso de equipamentos de informática, de sistemas de informação, da rede de comunicações e de continuidade do negócio do IFCE.

CAPÍTULO II

DAS PENALIDADES

Art. 32. O descumprimento ou violação da Política de Segurança da Informação poderá resultar na aplicação das sanções administrativas e/ou legais previstas na legislação vigente, conforme avaliação e orientação do GTSI.

Art. 33. Os casos omissos serão analisados e deliberados pelo GTSI do IFCE.

Art. 34. É vedada qualquer ação que não esteja explicitamente permitida na Política de Segurança do IFCE ou que não tenha sido previamente autorizada pelo GTSI.

CAPÍTULO III

DA APLICAÇÃO E VIGÊNCIA

Art. 36. A Política de Segurança da Informação deve ser revisada e atualizada periodicamente, ou sempre que ocorrerem eventos ou fatores relevantes que exijam sua revisão imediata.

Art. 37. Esta Norma é de aplicação interna e entra em vigor na data de sua publicação.

INSTITUTO FEDERAL
Ceará

INSTITUTO FEDERAL
Ceará

ANEXO I

TERMO DE RESPONSABILIDADE

Eu, , declaro que me comprometo a:

a) Acessar a Internet/Intranet somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Política de Segurança da Informação que rege o acesso à rede, à Internet/Intranet e a utilização de e-mails, especialmente no que tange aos Art. 17, Art. 20 e Art. 23 da Política de Segurança da Informação do IFCE;

b) Utilizar a caixa postal (e-mail) colocada a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na instrução normativa que rege o acesso à Internet/Intranet e utilização de e-mails, sem liberar o acesso a outras pessoas não envolvidas nos trabalhos executados, o que constitui descumprimento de normas legais, regulamentares e quebra de sigilo funcional;

c) Não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

d) Manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

e) Não me ausentar da estação de trabalho sem bloqueá-la com senha, garantindo assim a impossibilidade de acesso indevido por terceiros;

f) Não revelar minha senha de acesso de login de rede, de e-mail e/ou de sistemas de informação e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento, alterando- a utilizando números, letras maiúsculas e minúsculas assim que perceber que a mesma pode ter sido descoberta;

g) Responder, em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Declaro, ainda, estar plenamente esclarecido e consciente que:

INSTITUTO FEDERAL
Ceará

INSTITUTO FEDERAL
Ceará

1) É minha responsabilidade cuidar da integridade, confidencialidade e disponibilidade das informações sob minha guarda ou uso, devendo comunicar por escrito ao IFCE e à minha chefia imediata quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas nos sistema de informação ou recursos de rede, sendo proibida a exploração de falhas ou vulnerabilidades porventura existentes;

2) Não instalar, sob nenhuma hipótese, qualquer software em equipamentos da instituição, sendo a instalação de softwares e/ou similares, em dispositivos da instituição, de competência exclusiva do setor de TI;

3) Devo respeitar as normas de segurança e restrições de sistema impostas pelos sistemas de segurança implantados na instituição;

4) Devo cumprir e fazer cumprir os dispositivos da Política de Segurança da Informação do IFCE, de suas diretrizes, bem como deste Termo de Responsabilidade.

Constitui infração funcional e penal, enviar ou facilitar o envio por terceiros de e-mails falsos, inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos dos sistemas ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano; bem como modificar ou alterar o sistema de informações ou programa de informática sem autorização ou sem solicitação de autoridade competente ficando o infrator sujeito a punição com a demissão, conforme responsabilização por crime contra a Administração Pública, tipificado no art. 313-A e 313-B, do Código Penal Brasileiro (Decreto-Lei 2.848, de 1940).

Declaro, nesta data, ter ciência e estar de acordo com os procedimentos acima descritos, comprometendo-me a respeitá-los e cumpri-los plena e integralmente, além de manter sempre verossímeis os dados da instituição e de minha área de competência.

Local e Data

_____, _____ de _____ de 20_____.

_____ _____

Assinatura do colaborador

Representante Recursos Humanos