MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TOCANTINS
REITORIA

POLÍTICA DE GESTÃO DE REGISTROS (LOGS) DE AUDITORIA

Estabelece a Política de Gestão de Registros (logs) de Auditoria no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO).

CAPÍTULO I
DO ESCOPO

Art. 1° A Política de Gestão de Registros (*logs*) de Auditoria tem o objetivo de estabelecer diretrizes, competências e responsabilidades para governar o ciclo de vida da gestão dos registros (*logs*) de auditoria no âmbito do IFTO, garantindo assim que os *logs* sejam criados e analisados adequadamente.

Art. 2° Esta política se aplica aos ativos de TI do IFTO, incluindo servidores, estações de trabalho, *switches*, roteadores, access point, sistemas operacionais, banco de dados, servidores de arquivos, sistemas de informação e demais recursos e serviços de TI.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 3° Para fins de compreensão dos termos utilizados neste documento serão utilizadas as seguintes conceitos e definições:

I - ameaça: conjunto de fatores externos com o potencial de causar em dano para um sistema ou organização;

II - atividade: ação ou conjunto de ações executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

III - ativo: tudo que tenha valor para a organização, material ou não;

IV - ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

V - *backup/cópia de segurança:* conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

VI - banco de dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

VII - Comitê de Segurança da Informação (CSI): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

VIII - computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN);

IX - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

X - controles de segurança: certificado que autoriza uma pessoa natural para o tratamento de informação classificada;

XI - criptografia: arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

XII - CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

XIII - descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XIV - documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;

XV - e-mail: sigla de correio eletrônico (*electronic mail*);

XVI - eliminação: exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado;

XVII - Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade. Anteriormente era chamada de Equipe de Tratamento de Incidentes de Rede;

XVIII - evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

XIX - evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

XX - *firewall*: ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de hardware ou software, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo *firewall*, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

XXI - incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de

informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXII - incidente cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema;

XXIII - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXIV - informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXV - internet: rede global, composta pela interligação de inúmeras redes. Conecta mais de 500 milhões de usuários, provendo comunicação e informações das mais variadas áreas de conhecimento;

XXVI - medidas de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

XXVII - política de segurança da informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação. Este termo substituiu o termo Política de Segurança da Informação e Comunicação;

XXVIII - prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

XXIX - rede de computadores: conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

XXX - risco: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

XXXI - risco de segurança da informação: risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXXII - serviços: meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

XXXIII - SI: sigla de segurança da informação;

XXXIV - sistema de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

XXXV - tecnologia da informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações; e

XXXVI - usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da administração pública federal, formalizada por meio da assinatura de Termo de Responsabilidade.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 4° Esta política considera os seguintes princípios:

I - respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a administração pública federal;

II - garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do IFTO, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;

III - alinhamento estratégico da Política de Segurança da Informação com os demais planos institucionais;

IV - responsabilidade pelo cumprimento das normas pertinentes à segurança da informação vigentes; e

V - conscientização, educação e comunicação como alicerces fundamentais para o fomento da cultura em segurança da informação.

CAPÍTULO IV
DAS DIRETRIZES GERAIS

Art. 5° As diretrizes gerais constituem os pilares da gestão de registro de *logs* de auditoria no IFTO, norteando a elaboração de normas, planos, procedimentos, metodologias, ações e controles que garantem que os princípios de segurança da informação definidos na política de segurança da informação sejam atingidos.

§ 1º Registros (*logs*) de auditoria de eventos contendo atividades dos usuários, exceções e outros eventos de segurança da informação devem ser produzidos e mantidos por um período de tempo acordado com a ETIR para auxiliar em futuras investigações e monitoramento de controle de acesso.

§ 2º A atividade de auditoria de recursos, sistemas de informação e serviços de TI é de competência da área de Tecnologia da Informação do IFTO.

§ 3º Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de segurança da informação, tais como: autenticação, tanto as bem sucedidas quanto as malsucedidas, acesso a recursos e dados privilegiados e acesso e alteração nos registros de auditoria.

§ 4º As atividades dos administradores e operadores do sistema devem ser registradas e analisadas criticamente em intervalos regulares.

§ 5º Os serviços críticos contemplados nesta política devem ser formalmente elencados pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos.

§ 6º Procedimentos para o monitoramento do uso dos recursos de processamento da informação devem ser estabelecidos e os resultados das atividades de monitoramento devem ser analisados criticamente de forma regular.

§ 7º A equipe ETIR responsável pela auditoria interna de recursos, sistemas e serviços deve se reportar quando necessário ao Comitê de Segurança da Informação.

§ 8º A equipe responsável pela auditoria interna deve possuir capacidade técnica e experiência nas áreas de gerenciamento de *logs*, dispor de competências técnico-administrativas necessárias ao bom desempenho de suas funções quais sejam: independência, autonomia, imparcialidade, zelo, integridade e ética profissional, além de autoridade para avaliar as funções próprias e as funções terceirizadas do IFTO.

§ 9º É dever dos responsáveis pelos setores cooperarem com a ETIR quanto ao acesso a ativos de informação, instalações e transito de dados.

§ 10º Os membros da ETIR devem ter canal de comunicação permanente com os responsáveis pelos setores, para apoiar na atuação corretiva, de forma apropriada e tempestiva, em resposta às recomendações decorrentes dos trabalhos de auditoria.

CAPÍTULO V

GESTÃO DE REGISTRO DE (LOGS) DE AUDITORIA

Art. 6° O processo de gestão de registro de *logs* de auditoria deve gerenciar o ciclo de vida dos eventos realizados em recursos, sistemas, *softwares*, aplicativos, banco de dados, sistemas de informação e serviços de TI conforme determina a legislação pertinente.

Parágrafo Único. Este processo é composto por um conjunto de fases e atividades responsáveis pela coleta, armazenamento, uso e eliminação de eventos de segurança da informação que podem ajudar a detectar, compreender e recuperar-se de um ataque cibernético.

Seção I
Da coleta

Art. 7° A coleta de *logs* de auditoria registra os eventos realizados pelos usuários nos ativos de TI. Os logs são gerados por diversas fontes, incluindo software de segurança, antivírus, firewalls e sistemas de prevenção e detecção de intrusão, sistemas operacionais em servidores, estações de trabalho e equipamentos de rede e aplicações.

§ 1º A geração de *logs* de auditoria de eventos realizados pelos usuários deve estar habilitada nos ativos de informação, seguindo as diretrizes do processo de gestão de registros de *logs* de auditoria.

§ 2º *Logs* e registros de auditoria de ativos de informação devem ser coletados e retidos na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

§ 3º Quando possível *logs* devem ser coletados em um ou mais repositórios centrais.

§ 4º Ativos de informação classificados como críticos devem ter *logs* de auditoria registrados conforme legislação pertinente.

§ 5º Quando possível ativos de informação *do* IFTO devem gerar registros de *logs* auditoria para eventos definidos. Esses eventos definidos incluem a identificação de eventos significativos relevantes para a segurança da informação que precisam ser auditados.

§ 6º Os ativos de TI considerados críticos para o IFTO devem ter registrados os eventos de: tentativas de logon (do sistema ou domínio) bem-sucedidas e malsucedidas, gerenciamento de contas de usuários, acesso ao serviço de diretório, uso privilegiado, acompanhamento de processos, sistema e destruir arquivo de *logs* de auditoria.

§ 7º Ativos de informação que contêm dados sensíveis devem possuir os *logs* de auditoria que contenham dados sensíveis devem ter registros de eventos que permitam ajudar em uma eventual investigação forense, como por exemplo: identificação inequívoca do usuário que acessou o recurso; natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc; data e hora do evento; e endereço IP, identificador do ativo de informação e outras informações que possam identificar a possível origem do evento.

§ 8º Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (Logs) em formato que permita a completa identificação dos fluxos de dados.

Seção II
Do armazenamento

Art. 8° O IFTO na medida do possível deve centralizar a retenção de *logs* de auditoria de eventos realizados pelos usuários em seus ativos de informação com o objetivo de aperfeiçoar o gerenciamento destes *logs*.

§ 1º Ao definir o período de retenção de *logs* deve-se observar a definição legal de tempo de retenção/guarda/arquivamento de documentos e/ou dos dados tratados pelo IFTO.

§ 2º Os ativos de informação devem ser configurados de forma a armazenar seus registros de auditoria não apenas localmente, como também remotamente, por meio do uso de tecnologia aplicável, quando possível.

§ 3º Quando houver necessidade de transferência de *logs* para armazenamento alternativo deve-se proteger a confidencialidade e integridade dos registros de auditoria.

§ 4º No caso de os *logs* armazenados contiverem dados pessoais, deve-se observar o previsto pela Lei LGPD, a fim de avaliar se os *logs* devem ser eliminados ou conservados após o término do tratamento dos dados pessoais.

§ 5º Registros de *logs* auditoria devem ser retidos conforme previsto na legislação no âmbito da administração pública federal.

§ 6º Os registros de *logs* de auditoria e outros *logs* de eventos de segurança devem ser revisados e retidos de maneira segura.

§ 7º A capacidade de armazenamento dos *logs* deve ser constantemente verificada e readequada conforme a necessidade do IFTO.

§ 8º Registros de auditoria devem ser correlacionados quando houver mais de um repositório de *logs* ou coletados de várias fontes de *logs*.

§ 9º Cópias de segurança (backups) de arquivos de trilhas de auditoria de *logs* devem ser armazenados de forma segura, conforme legislação pertinente.

§ 10º Quando possível os registros devem ser armazenados conforme legislação pertinente no âmbito da administração pública federal.

Seção III
Do uso

Art. 9° O IFTO deve garantir que os *logs* de auditoria estejam disponíveis para o acesso quando for necessário, e manter o controle de acesso lógico aos diretórios onde os logs estão armazenados.

§ 1º O IFTO deve estabelecer um processo de análise de logs de eventos de auditoria de ativos de TI considerados críticos pela ETIR de forma proativa com o objetivo de detectar possíveis anomalias de comportamento dos ativos de informação.

§ 2º A frequência, escopo e/ou profundidade da revisão, análise e relatório dos registros de auditoria devem ser ajustados para atender às necessidades do IFTO com base nas informações recebidas.

§ 3º Análises de *logs* de auditoria de eventos devem ser realizadas pelo menos uma vez por semana, quando possível para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial.

§ 4º Processos, procedimentos e medidas técnicas devem ser definidas, implementadas e avaliadas para reporte de anomalias e falhas do sistema de monitoramento e notificação imediata ao responsável, caso confirmado.

§ 5º Eventos relacionados à segurança nos aplicativos e na infraestrutura subjacente devem ser identificados e monitorados.

§ 6º *Logs* e registros de auditoria de sistemas devem ser configurados e armazenados na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

§ 7º Em casos de resposta a incidentes cibernéticos, a coleta de dados forenses deve ser utilizada nos sistemas afetados, garantindo a transferência e a proteção de tais dados.

§ 8º Componentes do sistema e a operação desses componentes devem ser monitorados em busca de anomalias que sejam indicativas de atos maliciosos, desastres naturais e erros que afetem a capacidade do IFTO de atingir seus objetivos. As anomalias devem ser analisadas para determinar se representam eventos ou incidentes de segurança.

§ 9º Quando apropriado, *logs* de auditoria de consultas DNS e URL em ativos de informação devem ser coletados.

§ 10º As implementações de coleta de *logs* podem incluir a coleta de *logs* de auditoria de linhas de comando (CLI) tais como PowerShell, BASH e terminais administrativos remotos.

§ 11º O comportamento dos ativos de informação deve ser analisado para detectar e mitigar a execução de comandos e scripts que possam indicar ações maliciosas.

§ 12º Quando apropriado, *logs* do provedor de serviços devem ser coletados.

§ 13º Quando suportado, convém que o acesso a sistemas críticos por terceiros seja monitorado quanto a atividades não autorizadas ou incomuns.

§ 14º Processos de revisão, análise e relatórios de registros de auditoria devem ser correlacionados, para investigação e resposta a indicações de atividades ilegais, não autorizadas, suspeitas ou incomuns.

Seção IV
Da exclusão

Art. 10° Os eventos de auditoria em ativos de TI considerados críticos devem ser armazenados por um período pré-estabelecido e quando este prazo vencer, o IFTO deve ser capaz de realizar a eliminação de *logs* de forma eficiente, com base nas melhores práticas de segurança da informação e normativos como LGPD e LAI.

§ 1º A exclusão regular de logs de auditoria de eventos considerados desnecessários deve reduz a quantidade de dados que precisam ser filtrados para atender às requisições de resgate de informações além de reduzir os custos de armazenamento e gerenciamento de dados.

§ 2º Quando não forem mais necessários para requisitos legais, regulatórios (incluindo federais, estaduais e municipais) ou de negócios *do IFTO*, os dados de *logs* devem ser eliminados dos registros usando um método seguro aprovado.

§ 3º Quando possível deve-se implementar medidas de salvaguarda para os *logs*, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto, de forma que esses não tenham permissão de exclusão ou desativação dos registros (*logs*) de suas próprias atividades.

§ 4º A exclusão de logs de auditoria de eventos deve ser feita de modo a assegurar a irrecuperabilidade, destruindo inclusive as cópias, mídias digitais, impressos e discos rígidos.

CAPÍTULO VI
DO PLANO DE REGISTROS DE AUDITORIA

Art. 11° O plano de registros de logs de auditoria de eventos deve minimamente observar as seguintes diretrizes:

I - ativos de TI considerados críticos para o IFTO devem estar com as informações de data e hora sincronizadas. Pelo menos duas fontes de tempo devem ser configuradas para sincronizar o tempo dos ativos de informação, onde haver suporte;

II - ativos de informação do IFTO devem ser configurados de forma a sincronizar data e hora via protocolo NTP (*Network Time Protocol*), onde houver suporte;

III - em caso de incidentes de segurança da informação, ou quaisquer outros eventos de segurança, a ETIR deve coletar e preservar todos os registros de eventos do sistema operacional, serviço de TI, sistema de informação ou ativo de informação;

IV - a estrutura original de diretórios, incluindo todos os metadados associados, como data, hora de criação e atualização, e permissões dos arquivos deve ser mantida, para garantir a integridade das evidências;

V - em caso de impossibilidade de preservar as evidências do evento de segurança, o responsável pela área de TI deve justificar em relatório, a falta destas evidências.

CAPÍTULO VII
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I

Da Alta Administração

Art. 12° Compete à alta administração:

I - prover a orientação e o apoio necessário às ações de segurança da informação, de acordo com os objetivos estratégicos, planos institucionais, estrutura organizacional e com as leis e regulamentos pertinentes; e

II - garantir recursos (humanos, tecnológicos e financeiros) para a execução de ações relacionadas ao registro de logs de auditoria no âmbito do IFTO.

Seção II

Do Comitê de Segurança da Informação

Art. 13° Compete ao Comitê de Segurança da Informação:

I - deliberar sobre política e norma interna complementar de registro de *logs* de auditoria;

II - assessorar a implementação das ações para o registro de *logs* de auditoria; e

III - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre registro de *logs* de auditoria.

Seção III

Da Equipe de Tratamento e Resposta a Incidentes Cibernéticos

Art. 14° Compete à Equipe de Tratamento e Resposta a Incidentes Cibernéticos:

I - avaliar o processo de gestão de registro de *logs* de auditoria;

II - deliberar sobre procedimentos internos para registro de *logs* de auditoria; e

III - propor diretrizes e responsabilidades para a gestão de registro de *logs* de auditoria.

Seção IV

Do Gestor de Tecnologia da Informação

Art. 15° Compete ao Gestor de Tecnologia da Informação:

I - planejar, implementar e melhorar continuamente os controles de registro de *logs* de auditoria em soluções de tecnologia da informação e comunicações, nos termos da legislação vigente na Administração Pública Federal; e

II - propor diretrizes e responsabilidades para o registro de *logs* de auditoria.

Seção V

Do Gestor de Segurança da Informação

Art. 16° Compete ao Gestor de Segurança da Informação:

I - coordenar a elaboração da política e norma interna complementar sobre registro de logs de auditoria, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

II - assessorar a alta administração na implantação da Política de Gestão de Registros (*logs*) de Auditoria e das normas internas de segurança da informação do IFTO;

III - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à registros de *logs* de auditoria;

IV - propor recursos necessários às ações de registros de *logs* de auditoria;

V - verificar os resultados dos trabalhos de auditoria sobre a gestão de registros de *logs* de auditoria; e

VI - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos relacionados à gestão de registros de *logs* de auditoria.

Seção VI

Da Diretoria e demais setores de Tecnologia da Informação nas unidades do IFTO

Art. 17° Compete à Diretoria e demais setores de TI nas unidades do IFTO:

I - identificar os recursos, sistemas e serviços de TI que terão *logs* de auditoria gerenciados de acordo com a sua criticidade;

I - pesquisar, implantar e manter soluções para gestão de registro de *logs* de auditoria no âmbito do IFTO;

II - propor e gerenciar procedimentos de gestão de registro de *logs* de auditoria para a rede de comunicação de dados do IFTO;

III - implantar, configurar, gerenciar e monitorar a estrutura de registro de *logs* de auditoria;

IV - implementar rotinas para gestão de *logs* de auditoria; e

V - definir o fluxo do processo de gestão de *logs* de registro de auditoria.

Seção VII

Dos Usuários

Art. 18° Compete aos usuários:

I - atender aos princípios e diretrizes contidos nesta política, incluindo normas e procedimentos complementares destinados à segurança da informação e comunicação; e

II - guiar-se pelos princípios de confidencialidade, autenticidade, integridade, não repúdio, conformidade, controle de acesso e disponibilidade no decorrer de suas atividades.

CAPÍTULO VIII
DAS PENALIDADES

Art. 19° Ações que violem esta política, norma interna complementar, procedimentos, ou que quebrem os controles de segurança da informação serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

Parágrafo único. Casos omissos não tratados nesta política serão submetidos ao Comitê de Segurança da Informação.

CAPÍTULO IX
DA REVISÃO E ATUALIZAÇÃO

Art. 20° Esta política bem como a norma interna complementar gerada a partir dela deverão ser revisadas, aprovadas e atualizadas em função de alterações nas normativas do IFTO,

legislação pertinente, diretrizes e políticas do governo federal ou quando considerada necessária pelo Comitê de Segurança da Informação.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 21° As regras, medidas, controles e ações a serem executados nos procedimentos operacionais padrão para registro de *logs* de auditoria serão apresentados em norma interna complementar, alinhados às diretrizes emanadas pelo Comitê de Segurança da Informação e aos respectivos planos institucionais do IFTO.

Art. 22° Esta política e suas atualizações, bem como norma interna complementar, deverão ser divulgadas amplamente a todos os usuários, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Art. 23° A alta administração deverá disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução das diretrizes contidas nesta política.

Art. 24° Esta política entra em vigor a partir da data de sua publicação.

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 19/12/2023, às 10:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Kleyton Matos Moreira**, **Diretor**, em 22/12/2023, às 16:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2222394** e o código CRC **ABDF6F00**.

Avenida Joaquim Teotônio Segurado
Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul
CEP 77020-450 Palmas - TO
(63) 3229-2200
www.ifto.edu.br - reitoria@ifto.edu.br

Referência: Processo nº 23235.019035/2023-69 SEI nº 2222394