Modelo de Política de Gestão de Registros (Logs) de Auditoria

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 2.0

Brasília, março de 2023

MODELO DE POLÍTICA DE GESTÃO DE REGISTROS (LOGS) DE AUDITORIA

MINISTÉRIO DA GESTÃO E INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Sousa Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PROTEÇÃO DE DADOS

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Proteção de Dados

Equipe Técnica de Elaboração

Francisco Magno Felix Nobre

Ivaldo Jeferson de Santana Castro

Raphael César Estevão

Equipe Técnica de Revisão – Versão 2.0

Julierme Rodrigues da Silva

Raphael César Estevão

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
31/08/2022	1.0	Modelo de Política de Gestão de Registros (Logs) de Auditoria	Equipe Técnica de Elaboração
31/03/2023	2.0	Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo II.	Equipe Técnica de Revisão

Sumário

Aviso Preliminar e Agradecimentos

O presente Modelo, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na Elaboração de uma Política de Gestão de Registros (Logs) de Auditoria, em atendimento ao previsto no art. 46 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, deve adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito dos dados que estão sob sua custódia. Adicionalmente, a Elaboração de uma Política de Gestão de Registros (Logs) de Auditoria visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do Center for Internet Security (CIS), da International Organization for Standardization (ISO) e do National Institute of Standards and Technology (NIST). Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica da Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;
b) não se manifesta em nome de autoridades de privacidade e segurança da informação;
c) não é coautora das publicações internacionais abordadas;
d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente modelo; e
e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção “Referência Legal e de Boas Práticas” deste documento.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração deste documento.

Este Modelo será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas neste documento.

Introdução

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a elaborar sua Política de Registro (Logs) de Auditoria no âmbito institucional.

Os Controles 3 e 8 do Guia do Framework de Privacidade e Segurança da Informação (p. 46) estabelecem que:

Controle 3: Proteção de Dados *– Utilizar processos e ferramentas para identifcar, classificar, manusear, reter e descartar dados.*

Controle 8: Gestão de Registros de Auditoria *– Coletar, alertar, analisar e reter logs de eventos com objetivo de ajudar a detectar, compreender ou se recuperar de um ataque.*

O presente documento serve como um modelo prático a ser utilizado para auxiliar na adoção dos Controles 3 e 8 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas dos Controles 3 e 8 que estão contempladas por este Modelo de Política são: 3.3, 3.4, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.9, 8.10, 8.11 e 8.12.

Hoje, mais do que em qualquer outro momento da história, o Governo utiliza a tecnologia para melhorar e expandir a oferta de serviços públicos para o cidadão apoiado em sistemas informatizados.

Nesse contexto, os órgãos federais, com infraestrutura própria ou contratada de terceiros, coletam, recebem, acessam, processam, modificam, produzem, extraem, validam, armazenam, distribuem e transmitem informações confidenciais e públicas para apoiar a entrega de produtos e serviços essenciais (por exemplo, fornecimento de serviços financeiros; fornecimento de serviços de emissões guias, certificados e carteiras; processamento de autorizações de segurança ou dados de saúde; fornecimento de serviços em nuvem; desenvolvendo comunicações via cabo, wireless e/ou satélites; sistemas militares de defesa). As informações federais são frequentemente fornecidas ou compartilhadas, obedecidos os requisitos legais, com entidades como governos estaduais e municipais, empresas públicas e privadas, faculdades e universidades, organizações de pesquisa independentes ou públicas e organizações do terceiro setor.

A proteção dessas informações pelo Governo enquanto agente de tratamento está designada no **art. 46 da Lei Geral de Proteção de Dados**, sancionada em 14 de agosto de 2018:

> *"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."*

Importante ressaltar que adoção deste modelo não dispensa o órgão de considerar as diretrizes gerais estabelecidas para implementação da Política de Segurança da Informação, conforme prevê o art.12, Inciso IV

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 02/03/2023.

da Instrução Normativa Nº 01/GSI/PR, bem como os Capítulos III e IV da Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021, a qual dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.

Muitos logs dentro de um órgão ou entidade contém registros relacionados à segurança dos ativos de informação. Esses logs são gerados por muitas fontes, incluindo software de segurança, como software antivírus, firewalls e sistemas de prevenção e detecção de intrusão; sistemas operacionais em servidores, estações de trabalho e equipamentos de rede; e aplicações. O gerenciamento desses logs é essencial para garantir que os registros sejam coletados, armazenados, usados e excluídos, com detalhes suficientes por um período apropriado. A análise de log de rotina é benéfica para identificar incidentes, violações de política, atividades fraudulentas e problemas operacionais. Os logs também são úteis ao realizar auditorias e análises forenses, dar suporte a investigações internas, estabelecer linhas de base e identificar tendências operacionais e problemas de longo prazo.

A política de gestão de registros (logs) de auditoria fornece os processos e procedimentos para governar o ciclo de vida da gestão dos registros (logs) de auditoria, garantindo assim que os logs sejam criados e analisados adequadamente. Esta política se aplica a todos os departamentos e todos os ativos conectados à rede corporativa.

A implementação das recomendações a seguir deve ajudar em um gerenciamento de logs mais eficiente e eficaz para as instituições públicas.

Política de Gestão de Registros (Logs) de Auditoria – PGRA

IMPORTANTE: Este modelo de Política de Gestão de Registros (Logs) de Auditoria – PGRA deve ser utilizado exclusivamente como referência, devendo o órgão ou entidade considerar as particularidades técnicas específicas do seu ambiente, bem como observar a boa aderência aos processos internos, a fim de construir uma política que seja adequada a sua realidade.

Este modelo tem por foco prover diretrizes para Política de Gestão de Registros (Logs) de Auditoria – PGRA. Contudo, recomenda-se que o órgão ou entidade considere, no mínimo, as diretrizes gerais estabelecidas para implementação da Política de Segurança da Informação, conforme prevê o art.12, Inciso IV da Instrução Normativa Nº 01/GSI/PR, bem como os Capítulos III e IV da Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021, a qual dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal.
Para usar este modelo, basta substituir o texto em cinza itálico por informações personalizadas do seu órgão ou entidade. Quando estiver concluído, exclua todos os textos introdutórios cinza não itálico ou de exemplo e converta todo o texto restante em preto antes do processo de aprovação.

Responsável	*Nome da pessoa ou área responsável pela gestão desta política.*
Aprovado por:	*Nome da pessoa ou área responsável pela aprovação e autorização da implementação desta política.*
Políticas relacionadas	*Relacione outras políticas corporativas relacionadas dentro ou externas a este modelo, por exemplo, Política de Gestão de Riscos \ Política de Backup e Restauração de Dados Digitais \ POSIN (Política de Segurança da Informação)*
Localização de armazenamento	*Descreva a localização física ou digital das cópias desta política.*
Data da aprovação	*Liste a data em que essa política entrou em vigor.*
Data de revisão	*Liste a data em que a política deve passar por revisão e atualização. Recomenda-se que seja definido um período de revisão da política, pelo menos um ano, ou quando houver alterações de normativos legais significativos sobre o tema.*

Propósito [Objetivo da Política] conforme IN01 GSI/PR art.11

Levando em consideração natureza e a finalidade do órgão ou da entidade, descreva os fatores ou circunstâncias que determinam a existência da Política de Gestão de Registros (Logs) de Auditoria – PGRA. Além disso, informe os objetivos básicos da política e o que ela pretende alcançar.

Exemplo: *O objetivo da Política de Gestão de Registros (Logs) de Auditoria – PGRA é estabelecer e manter um processo de gestão de log de auditoria que defina os requisitos de log do órgão ou entidade. Tal processo deve tratar da coleta, armazenamento, uso e exclusão de logs de auditoria e sistemas para os ativos de informação [do órgão ou entidade]. É importante que seja estabelecida a revisão periódica deste processo de gestão de log de auditoria.*

Definir os princípios de atuação da auditoria interna nos processos de TI [do órgão ou entidade] e as diretrizes para a administração e gerenciamento de registros de logs gerados pelos ativos de informação.

Escopo [Amplitude, alcance da Política] conforme IN01 GSI/PR art.12 item I

Defina a quem e a quais sistemas esta política se aplica. Liste os agentes públicos e colaboradores necessários para cumprir ou simplesmente indique "todos" se todos devem cumprir. Também indique quaisquer exclusões

ou exceções que estejam fora de escopo, ou seja, essas pessoas, elementos ou situações que não estejam cobertas por esta política ou onde uma consideração especial possa ser feita.

Esta **Política de Gestão de Registros (Logs) de Auditoria – PGRA** se aplica aos ativos informacionais *[do órgão ou entidade]*, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e ou os utilize.

Os serviços de TI críticos *[do órgão ou entidade]* devem ser formalmente elencados pelo *[citar o responsável pela definição, ex.: Comitê de Gestão de Tecnologia da Informação do órgão ou entidade].*

A seguir são consideradas duas opções de texto, uma para caso o órgão já possua o mapeamento dos sistemas críticos e outra para caso o órgão não possua esse documento de mapeamento dos sistemas críticos.

Opção 1:

Já ficam previamente estabelecidos como serviços e sistemas críticos do *[órgão ou entidade]* os relacionados em *[nome do documento que possui a seleção de sistemas críticos]*.

Opção 2:

Já ficam previamente estabelecidos os *[citar tipo ou nome dos processos ou sistemas críticos]*, como serviços críticos do *[órgão ou entidade]*.

O *[departamento/coordenação de TI do órgão ou entidade]* é responsável por elaborar, manter e fazer cumprir a Política de Gestão de Registros (Logs) de Auditoria – PGRA *[no órgão ou entidade].*

Exceções

Podem ocorrer de alguns ativos de informação *[do órgão ou entidade]* não serem contemplados por possíveis dificuldades técnicas ou obrigações contratuais e normativas. Quaisquer exceções a esta política deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções *[do órgão ou entidade].*

É importante salientar que tais exceções precisam ser tratadas no mapeamento de riscos de segurança da informação que o órgão ou a entidade deve efetuar em cumprimento ao Capítulo III da Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021.

Público

Esta Política de Gestão de Registros (Logs) de Auditoria – PGRA se aplica aos ativos informacionais *[do órgão ou entidade]*, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e ou os utilize, com responsabilidades específicas a indivíduos atuantes na gestão, processo e desenvolvimento em nome *[do órgão ou entidade]*. Além disso, essa política se aplica, nos limites estabelecidos contratualmente, a quaisquer provedores e entidades terceirizadas com acesso aos ativos de informação *[do órgão ou entidade]*.

Termos e definições [Glossário] conforme PORTARIA GSI/PR Nº 93

Defina quaisquer termos-chave, siglas ou conceitos que serão utilizados na política. [Sugere-se utilizar como referência as definições apresentadas na PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021 – Glossário de Segurança da Informação do Gabinete de Segurança Institucional da PRESIDÊNCIA DA REPÚBLICA]. Exemplo:

ATIVO **-** Qualquer coisa que tenha valor para a organização.

ATIVO DE REDE - Equipamento que centraliza, interliga, roteia, comuta, transmite ou concentra dados em uma rede de computadores.

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.

DESCARTE - eliminação correta de informações, documentos, mídias e acervos digitais.

ETIR - Sigla de Equipe de Prevenção, Tratamento, e Resposta a Incidentes Cibernéticos.

EVENTO - Qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Ou seja, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao usuário.

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.

HOST - Um computador ou dispositivo de TI (por exemplo, roteador, switch, gateway, firewall).

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.

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. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não-autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não-autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não-autorizadas de firmware, hardware ou software em um ambiente computacional; d) ataques de negação de serviço (DoS); e demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada.

INCIDENTE DE SEGURANÇA – Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

LOG (REGISTRO DE AUDITORIA) – registro de eventos relevantes em um dispositivo ou sistema computacional.

LOG DE AUDITORIA – Fornecem eventos no nível do sistema que mostram vários horários de início/término de processo do sistema, travamentos etc. São nativos dos sistemas e exigem menos configurações para ativarem.

LOG DE SISTEMA – Incluem eventos no nível do usuário - quando um usuário faz login, acessa um arquivo etc.

NTP (Network Time Protocol) – Protocolo de Tempo para Redes.

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.

SANITIZAÇÃO DE DADOS - Eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados.

TRILHA DE AUDITORIA - registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento.

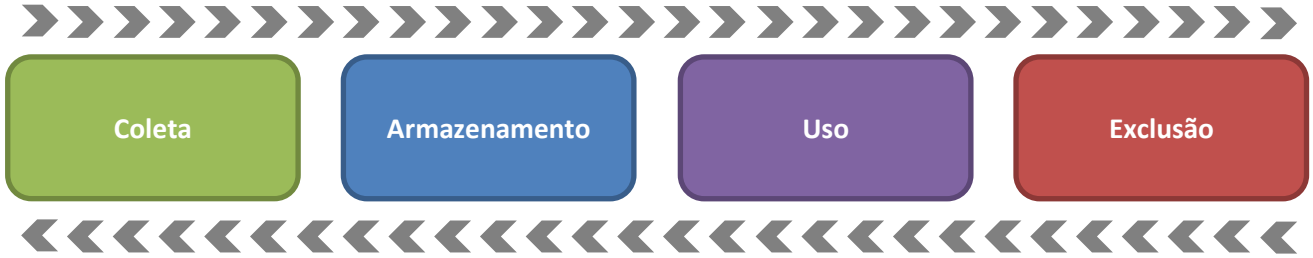
Referência legal e de boas práticas [Documentos norteadores]

Se for aplicável, liste quaisquer leis, regulamentos ou guias de boas práticas que regem a política ou com as quais a política deve estar em conformidade ou ser cumprida. Confirme com a consultoria jurídica que a lista é completa e precisa.

Orientação	Seção
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)	Anexo, art.3, Inciso I, II e V
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15
Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI;	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Guia do Framework de Privacidade e Segurança da Informação	Controles 3 e 8
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI;	Gestão da Segurança da Informação
Guias Operacionais SGD	Todos
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea g, h
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021	Capítulo IV
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II art. 50
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos;	A.12.3 Cópias de segurança
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;	12.3 Cópias de segurança 18 Conformidade
Norma Complementar nº 21/IN01/DSIC/GSIPR	Em sua íntegra
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra
Publicação do TCU sobre descarte de mídias, disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp%3FfileId%3D8A8182A25232C6DE0152A27D76A458D8&sa=U&ved=2ahUKEwiytu-c59_4AhV9uZUCHXFaBPgQFnoECAg	Em sua íntegra
Audit Log Management Policy Template for CIS Control 8	Em sua íntegra

Gestão de registros de auditoria

O documento é organizado em quatro fases, Coleta, Armazenamento, Uso e Exclusão. Dentro dessas fases foram inseridas medidas de segurança, todas oriundas do *Center for Internet Security* CIS, framework *Critical Security Control v8.0 Assessment Tool* - contidas no Controle 8 (*Audit Log Management*).



Cada fase compreende uma etapa do ciclo de vida de um log, seja esse log de auditoria ou um log de sistema. Importante ressaltar que se deve fazer cumprir a ordem das fases, pois se trata de uma ordem lógica, o mesmo não equivale para ordem das medidas encontradas no framework.

Todas as 12 medidas, encontradas no controle 8 do CIS foram divididas de acordo com as quatro fases (coleta, armazenamento, uso e exclusão). A inserção das medidas nas fases se deu conforme a orientação descrita pelo framework, ou seja, as medidas foram classificadas de acordo com a fase do ciclo de vida de um log.

Declarações da política [Regras aplicáveis ao caso específico]

Descreva as regras que compõem a política. Isso normalmente toma a forma de uma série de breves declarações prescritivas e proscritivas. A subdivisão desta seção em subseções pode ser necessária dependendo do comprimento ou complexidade da política. Exemplo:

Os sistemas e dispositivos conectados à rede do órgão ou entidade, sejas próprios ou suportados por terceiros, devem submeter-se a geração de registros e logs de auditoria.

Premissas e responsabilidades

1. A atividade de auditoria é de competência da *[equipe responsável, gestores de sistemas, área de tecnologia e prestadores de serviço] [do órgão ou entidade]*.
2. A equipe responsável pela auditoria interna deve se reportar ao *[definir o departamento de alta gestão] [do órgão ou entidade]*.
3. A *[equipe responsável]* 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 órgão ou entidade]*.
4. A *[equipe responsável pela auditoria]* pode obter assessoria de especialistas/consultores externos ou mesmo equipe terceirizada para subsidiar a área quando essa não for suficientemente proficiente.
5. A *[equipe responsável],* quando executa a atividade de auditoria, deve possuir acesso irrestrito às informações necessárias ao bom desempenho de suas funções, quais sejam: *[acesso irrestrito a quaisquer informações, ambientes e ativos de informação]*.
6. É dever dos *[coordenadores do órgão ou entidade]* cooperar com a *[equipe responsável]* quanto ao acesso a ativos de informação, instalações e trânsito de dados.
7. Os membros da *[equipe responsável]* pela auditoria devem ter canal de comunicação permanente com *[coordenadores do órgão ou entidade]*, para apoiar na atuação corretiva, de forma apropriada e tempestiva, em resposta às recomendações decorrentes dos trabalhos de auditoria.
8. Os eventos de log devem ser gerados, selecionados e armazenados para todos os ativos.

9. A *[equipe responsável]* deve selecionar os eventos e os respectivos tempos de guarda, bem como as demais características de uso dos eventos.

10. As exceções deverão ser documentadas.

Requisitos do plano de registros de auditoria

11. Ativos de informação 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 houver suporte.

12. Ativos de informação *[do órgão ou entidade]* devem ser configurados de forma a sincronizar data e hora via *[protocolo NTP (Network Time Protocol)]*, onde houver suporte.

13. *Utilizar o horário de Greenwich em sistemas hospedados em provedores de nuvem onde o fuso local pode ser diferente do fuso do provedor*

Implante e faça cumprir uma política de gestão de acesso, com o objetivo de estabelecer diretrizes quanto aos acessos bem-sucedidos e malsucedidos aos ativos de informação.

Estabeleça e faça cumprir uma política de gestão de ativos de informação, e a partir desta política, poderá definir quais os ativos de informação podem ser configurados para cumprir a Política de Gestão de Registros (Logs) de Auditoria – PGRA.

14. Processos, procedimentos e medidas técnicas devem ser definidos e implementados visando a proteção dos dados sensíveis ao longo de seu ciclo de vida.

15. Devem ser mapeados os ativos de informação que podem ter suas configurações de log mais detalhadas com informações como: *[ID de usuário de acesso, IP do host, data, hora e fuso horário, acessos de usuários privilegiados etc.]*.

16. Devem ser mapeados os ativos de informação, que por qualquer motivo, não possa apresentar dados detalhados conforme item 15.

17. Além de eventos em ativos de informação, *[o órgão ou entidade]* pode registrar eventos de segurança da informação como os a seguir:

    Exemplo:

    a) Utilização de usuários, perfis e grupos privilegiados;
    b) Acoplamento e desacoplamento de dispositivos de hardware, principalmente mídias removíveis;
    c) Inicialização, suspensão e reinicialização de serviços;
    d) Criação, modificação e exclusão de grupos ou listas de grupos com acessos privilegiados;
    e) Atualização das regras da política de senhas de usuários;
    f) Criação, acesso e modificação de arquivos de sistemas considerados críticos;
    g) Qualquer evento realizado nos ativos de informação de segurança existentes.

18. Em caso de incidentes de segurança da informação, ou quaisquer outros eventos de segurança, a(o) *[equipe responsável] [do órgão ou entidade]* deve coletar e preservar todos os registros de eventos citados no item 15 e as mídias de armazenamento dos ativos de informação afetados pelo evento.

19. Caso não seja possível cumprir com as diretrizes apontadas no item 15, em razão do reestabelecimento dos sistemas e serviços afetadas de forma rápida, a(o) *[equipe responsável] [do órgão ou entidade]* deve coletar e armazenar cópias dos registros e arquivos afetados pelo incidente de segurança como:

    Exemplo:

    a) Logs;
    b) Arquivos de sistema operacional;
    c) Configurações do sistema operacional; e

d) *Demais arquivos e logs que foram necessários para reestabelecimento do serviço ou sistema.*

20. O *[órgão ou entidade]* deve manter a estrutura original de diretórios além dos “metadados” destes arquivos tais como: *[data, hora de criação e atualização e permissões]*.
21. Em caso de impossibilidade de preservar as evidências do evento de segurança, o *[responsável pela ETIR]* deve justificar em relatório, a falta destas evidências.
22. As ações para o reestabelecimento do serviço e sistema afetados pelo evento de segurança não devem impossibilitar a coleta, a preservação e disponibilidade das evidências de forma integra.
23. Devem ser promovidas ações para a preservação dos arquivos coletados.

Fases da gestão de registros de auditoria

Segue o detalhamento das quatro fases do processo de gerenciamento de logs de auditoria, divididas em coleta, armazenamento, uso e exclusão.

Coleta

O órgão ou entidade deve ter a capacidade de realizar a coleta de logs de auditoria em todos os ativos de informação, isso implica aos administradores a configuração das fontes de log para capturar as informações necessárias no formato e local desejados. Esses logs são gerados por muitas fontes, incluindo software de segurança, como software antivírus, firewalls e sistemas de prevenção e detecção de intrusão; sistemas operacionais em servidores, estações de trabalho e equipamentos de rede; e aplicações.

Para melhorar o nível de maturidade desta atividade, é importante que o órgão ou entidade consiga coletar os logs de auditoria de forma detalhada, e tais logs tenham dados importantes como data, hora de criação, atualização, permissões, nome do usuário, origem do evento, endereços de origem, endereços de destino e outros elementos úteis que podem ajudar em uma investigação forense.

Ao coletar logs do provedor de serviço que tratam de dados pessoais deve-se observar as orientações contidas na LGPD e demais regulamentações de proteção de dados e privacidade.

A não observância da conformidade do item 0, pode acarretar prejuízos financeiros e reputacionais, além das sanções administrativas relacionadas no art. 52 da LGPD.

24. Em caso de incidente de segurança da informação, todo e qualquer material coletado deverá ser lacrado e custodiado pelo agente *[responsável pela ETIR]*, e este deve preencher um *[Termo de Custódia dos Ativos de Informação]* relacionados ao incidente de segurança. O material coletado ficará à disposição da autoridade comunicada, a qual orientará quanto a sua destinação.
25. A geração de log de auditoria deve estar habilitada nos ativos de informação, seguindo as diretrizes do processo de gestão de registros de auditoria *[do órgão ou entidade]*.
26. Logs e registros de auditoria de ativos de informação devem ser criados e retidos na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.
27. Logs devem ser coletados em um ou mais repositórios centrais.
28. Deve ser assegurado que ativos de informação classificados como críticos estejam registrando logs de auditoria.
29. Usuários e componentes dos ativos de informação devem ser monitorados continuamente em busca de comportamento anômalo ou suspeito.
30. Ativos de informação *[do órgão ou entidade]* devem gerar registros de auditoria para eventos definidos. Esses eventos definidos incluem a identificação de eventos significativos relevantes para a segurança da informação que precisam ser auditados.

A atividade de auditoria pode afetar o desempenho dos ativos de informação e esta questão deve ser considerada

como um fator separado durante sua aquisição. Os ativos de informação do órgão ou entidade devem produzir, a nível de software ou sistema operacional, registros de auditoria contendo informações suficientes para estabelecer quais eventos ocorreram, as fontes e os resultados de tais eventos.

31. A lista de eventos auditáveis definidos deve ser revisada e atualizada periodicamente, pelo menos a cada *[período]*.

32. Devem ser registrados os eventos de:

Exemplo:

a) tentativas de logon (do sistema ou domínio) bem-sucedidas e malsucedidas;
b) gerenciamento de contas de usuários;
c) acesso ao serviço de diretório;
d) uso privilegiado;
e) acompanhamento de processos;
f) sistema;
g) destruir arquivo de log de auditoria.

33. Entradas de trilha de auditoria para componentes do sistema podem ser registradas de forma classificada e personalizada.

Exemplo:

a) Identificação do usuário;
b) Tipo de evento;
c) Data e horário;
d) Indicação de sucesso ou falha;
e) Origem do evento;
f) A identidade ou o nome dos dados afetados, componentes do sistema ou recurso.

34. Ativos de informação que contêm dados sensíveis devem possuir log de auditoria detalhado, incluindo, mas não se limitando, a elementos úteis que possam ajudar em uma eventual investigação forense.

Exemplo:

a) Origem do evento;
b) Data e hora do evento;
c) Nome de usuário;
d) Endereços de origem e destino.

Armazenamento

O órgão ou entidade pode centralizar a retenção de logs em seus ativos de informação com o objetivo de aperfeiçoar o gerenciamento destes logs. Importante lembrar que deve ser capaz de armazenar os logs de auditoria seguindo diretrizes de segurança presentes nos artefatos normativos como a LGPD e a NC nº 21 /IN01/DSIC/GSIPR e demais referências de boas práticas.

Esteja ciente de que a alocação de capacidade de armazenamento de log suficiente reduz a probabilidade de tal capacidade ser excedida e resultar na perda ou redução potencial da capacidade de log.

Importante ressaltar que no momento de definir o período de retenção dos logs é indicado verificar:

- A existência de definição legal de tempo de retenção/guarda/arquivamento de documentos e/ou dos dados tratados pelo órgão e/ou entidade para os quais os logs foram gerados; e
- **Tabela de temporalidade do CONARQ**[2].

A transferência de logs, também conhecida como off-loading, é um processo comum em sistemas com capacidade limitada de armazenamento de logs e, portanto, oferece suporte à disponibilidade dos logs. O

[2] https://www.gov.br/arquivonacional/pt-br/servicos/gestao-de-documentos/orientacao-tecnica-1/codigo-de-classificacao-e-tabela-de-temporalidade-e-destinacao-de-documentos-de-arquivo/cod_classif_e_tab_temp_2019_m_book_digital_25jun2020_1.pdf

armazenamento de log inicial é usado apenas de forma transitória até que o sistema possa se comunicar com o sistema secundário ou alternativo alocado para armazenamento de log, momento em que os logs são transferidos. A transferência de logs para armazenamento alternativo, deve ser feita para um ativo de informação que esteja em uma rede lógica, ou física diferente, com o propósito de proteger a confidencialidade e integridade dos registros de auditoria, para isso, convêm que tal transferência seja realizada por meio de comunicação segura (criptografada).

35. O armazenamento de logs deve estar de acordo com o processo de gestão de logs *[do órgão ou entidade]*.
36. No caso de os logs armazenados contiverem dados pessoais, deve-se observar o previsto pelo art. 16 da LGPD a fim de avaliar se os logs devem ser eliminados ou conservados após o término do tratamento dos dados pessoais.
37. Registros de auditoria devem ser retidos por pelo menos *[período]*. Uma vez que o período mínimo de retenção tenha sido atingido, *[o órgão ou entidade]* pode continuar a reter registros de auditoria até que seja determinado que eles não sejam mais necessários para fins administrativos, legais, de auditoria ou outros fins operacionais.
38. Os registros de log de auditoria e outros logs de eventos de segurança devem ser revisados e retidos de maneira segura.

Busque implementar hardware, software e/ou mecanismos/procedimentos que registrem e examinem a atividade em ativos de informação que contenham ou usem informações de sensíveis.

Identificar e classificar problemas e suas causas-raiz fornecendo resolução oportuna pode ajudar a evitar incidentes recorrentes e recomendações para melhorias.

Exemplo:

Implementar trilhas de auditoria automatizadas para todos os componentes do sistema para reconstruir os seguintes eventos:

a) Todos os acessos de usuários individuais aos dados classificados como sensíveis;
b) Todas as ações desempenhadas por qualquer pessoa com privilégios root ou administrativos;
c) Acesso a todas as trilhas de auditoria;
d) Tentativas inválidas de acesso lógico;
e) Uso e as alterações dos mecanismos de identificação e autenticação, inclusive, entre outros, a criação de novas contas, aumento de privilégios e demais alterações, adições ou exclusões de contas com privilégios root ou administrativos;
f) Inicialização, interrupção ou pausa dos registros de auditoria;
g) Criação e exclusão de objetos a nível do sistema.

39. A capacidade de armazenamento dos logs deve ser constantemente verificada.
40. Registros de auditoria devem ser correlacionados quando houver mais de um repositório de logs ou coletados de várias fontes de logs.
41. Cópias de segurança (backups) de arquivos de trilhas de auditoria de log devem ser armazenados de forma segura, em mídia de difícil alteração.

Uso

O órgão ou entidade deve garantir que os logs estejam disponíveis para o acesso quando for necessário, e manter o controle de acesso lógico aos diretórios de logs. O órgão ou entidade pode estabelecer um processo de análise de logs de forma proativa com o objetivo de detectar possíveis anomalias de comportamento dos ativos de informação.

A revisão, análise e relatórios de registros de auditoria abrangem o registro relacionado à segurança e privacidade da informação realizado pelas instituições, incluindo o registro que resulta do monitoramento do uso da conta, acesso remoto, conectividade sem fio, conexão de dispositivo móvel, definições de configuração, inventário de componentes do sistema, uso de ferramentas de manutenção e manutenção não local, acesso

físico, entrega e remoção de equipamentos, comunicações nas interfaces do sistema e uso de código móvel ou Voice over Internet Protocol (VoIP). RETEN

As descobertas podem ser relatadas a entidades institucionais que incluem a equipe de resposta a incidentes, o suporte técnico e os departamentos de segurança e/ou privacidade. Caso as instituições estiverem proibidas de revisar e analisar registros de auditoria ou não puderem realizar tais atividades, a revisão ou análise poderá ser realizada por outras instituições que tenham essa autoridade.

42. A frequência, escopo e/ou profundidade da revisão, análise e relatório dos registros de auditoria devem ser ajustados para atender às necessidades *[do órgão ou entidade]* com base nas informações recebidas.
43. Análises de logs de auditoria devem ser realizadas pelo menos *[período]* para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial.
44. 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.
45. Eventos relacionados à segurança nos aplicativos e na infraestrutura subjacente devem ser identificados e monitorados.

Busque a implementação de sistema para gerar alertas direcionados às partes interessadas responsáveis com base em tais eventos e métricas correspondentes.

46. 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.
47. 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.

Exemplo de conteúdo que pode ser incluído em cada evento auditado:

a) *Data e hora do evento.*
b) *O componente do ativo de informação (por exemplo, componente de software, componente de hardware) onde ocorreu o evento.*
c) *Tipo de evento.*
d) *Identidade do usuário/sujeito.*
e) *Resultado (sucesso ou fracasso) do evento.*

48. 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 órgão ou entidade]* de atingir seus objetivos. As anomalias devem ser analisadas para determinar se representam eventos ou incidentes de segurança.
49. Quando apropriado, logs de auditoria de consultas DNS e URL em ativos de informação devem ser coletados.
50. 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.
51. O comportamento dos ativos de informação deve ser analisado para detectar e mitigar a execução de comandos e scripts que possam indicar ações maliciosas.
52. Quando apropriado, logs do provedor de serviços devem ser coletados.

Exemplo de implementações devem incluir a coleta de eventos de autenticação e autorização, eventos de criação e descarte de dados e eventos de gerenciamento de usuários.

53. Quando suportado, convém que o acesso a sistemas críticos por terceiros seja monitorado quanto a atividades não autorizadas ou incomuns.
54. 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.

Exclusão

Seguindo a política de gestão de logs da organização, é importante que os logs sejam armazenados por um período pré-estabelecido e quando este prazo vencer, a organização deve ser capaz de realizar a exclusão de logs de forma eficiente, com base nas melhores práticas de segurança da informação e normativos como LGPD e LAI.

Recomenda-se a utilização de técnicas de descarte, ou sanitização de dados durante o a fase de exclusão de dos logs.

A exclusão regular de dados considerados desnecessários também reduz a quantidade de dados que você precisa filtrar para atender às requisições de resgate de informações além de reduz os custos de armazenamento e gerenciamento de dados.

55. Quando não forem mais necessários para requisitos legais, regulatórios (incluindo federais, estaduais e municipais) ou de negócios *[do órgão ou entidade]*, os dados de logs devem ser removidos dos registros usando um método seguro aprovado.
56. 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 (log) de suas próprias atividades.
57. A exclusão deve ser feita de modo a assegurar a irrecuperabilidade, destruindo inclusive as cópias, mídias digitais, impressos e discos rígidos.

    Exemplo:

    a) Mídias digitais, como fita, CD/DVD e unidades flash, devem ser trituradas;
    b) Discos rígidos devem ser apagados usando um padrão recomendado para destruição de dados ou destruídos fisicamente;
    c) Cópias dos dados em sistemas ativos e de backup, devem ser destruídos fisicamente ou devem utilizar um padrão recomendado para destruição;
    d) Cópias impressas dos logs e relatórios em papel devem ser cortados em tiras (picotados) e incinerados;

58. No caso em que o descarte/exclusão for realizado por meio de terceiro, deve-se incluir registro/rastreamento quando enviado por correio seguro ou outro método de entrega.

Lembre-se que pode ser fácil apagar dados impressos, mas os dados digitais geralmente deixam um rastro e as cópias podem residir em servidores de arquivos e bancos de dados esquecidos.

59. Mídias digitais de armazenamento ou discos rígidos podem ser reutilizados, desde que seja realizada a sobrescrição de dados na mídia a ser reutilizada.

É importante ter atenção e cuidados com a sobrescrição de dados, utilize ferramentas adequadas durante a sobrescrição para não danificar a mídia e ou os dados anteriores não serem expostos de forma desnecessária.

Recomendações técnicas

Restringir a instalação de aplicativos e softwares. O privilégio de instalação de aplicativos e softwares deve ser restrito a indivíduos autorizados obedecendo os critérios do órgão ou entidade.

Desabilitar logs na nuvem. Agentes mal-intencionados podem desabilitar recursos e integrações de log na nuvem para limitar quais dados são coletados em suas atividades e evitar a detecção.

Desabilitar a inicialização TFTP (Trivial File Transfer Protocol). Agentes mal-intencionados podem abusar da inicialização pela rede para carregar um sistema operacional de dispositivo de rede não autorizado a partir de um servidor TFTP. A inicialização TFTP (netbooting) é comumente usada por administradores de rede para carregar imagens de dispositivos de rede controladas por configuração de um servidor de gerenciamento centralizado. A inicialização por rede é uma opção na sequência de inicialização e pode ser usada para

centralizar, gerenciar e controlar imagens de dispositivos.

Remover indicador no host – Agentes mal-intencionados podem excluir ou alterar artefatos gerados em um sistema host, incluindo logs ou arquivos capturados, como malware em quarentena. Os locais e o formato dos logs são específicos da plataforma ou do produto, no entanto, os logs do sistema operacional padrão são capturados como eventos do Windows ou arquivos Linux/macOS, como Bash History e /var/log/*.

Limpar logs de eventos do Windows – Agentes mal-intencionados podem limpar os logs de eventos do Windows para ocultar a atividade de uma intrusão. Os logs de eventos do Windows são um registro de alertas e notificações de um computador. Existem três fontes de eventos definidas pelo sistema: Sistema, Aplicativo e Segurança, com cinco tipos de eventos: Erro, Aviso, Informações, Auditoria de Sucesso e Auditoria de Falha.

Limpar logs do sistema Linux ou Mac - Agentes mal-intencionados podem limpar os logs do sistema para ocultar evidências de uma invasão. O macOS e o Linux acompanham as ações do sistema ou iniciadas pelo usuário por meio de logs do sistema. A maioria dos logs do sistema nativo é armazenada no diretório /var/log/. As subpastas neste diretório categorizam os logs por suas funções relacionadas, como:

a) **At (Linux)** - Agentes mal-intencionados podem abusar do utilitário at para realizar o agendamento de tarefas para execução inicial ou recorrente de código malicioso. O comando at nos sistemas operacionais Linux permite que os administradores programem tarefas.
b) **Launchd** - Agentes mal-intencionados podem abusar do daemon Launchd para realizar o agendamento de tarefas para execução inicial ou recorrente de código malicioso. O daemon launchd, nativo do macOS, é responsável por carregar e manter os serviços dentro do sistema operacional. Esse processo carrega os parâmetros para cada daemon de nível de sistema de inicialização sob demanda dos arquivos de lista de propriedades (plist) encontrados em /System/Library/LaunchDaemons e /Library/LaunchDaemons. Esses LaunchDaemons possuem arquivos de lista de propriedades que apontam para os executáveis que serão lançados.
c) **Cron** - Agentes mal-intencionados podem abusar do utilitário cron para realizar o agendamento de tarefas para execução inicial ou recorrente de código malicioso. O utilitário cron é um agendador de tarefas baseado em tempo para sistemas operacionais do tipo Unix. O arquivo crontab contém o agendamento das entradas cron a serem executadas e os tempos especificados para execução. Todos os arquivos crontab são armazenados em caminhos de arquivo específicos do sistema operacional.

Procedimentos relevantes

Considere criar documentos de procedimento formal que reforcem e apoiem as declarações políticas acima. Note que é uma prática recomendada abrigar políticas e procedimentos em documentos separados para manter o conteúdo focado e reduzir o número de vezes que a política deve ser reprovada pela alta administração.

ANEXO I

Mudanças da Versão 2.0

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Modelo de Política de Gestão de Registros (Logs) de Auditoria.

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam a adequação com o Guia do Framework de Privacidade e Segurança da Informação v1 elaborado e publicado pela SGD em novembro de 2022.

Foram realizadas inclusões de: seção sobre aviso preliminar e agradecimentos; referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Modelo de Política de Gestão de Registros (Logs) de Auditoria; e atualização da seção “Referência legal e de boas práticas”. Foram realizadas modificações, inclusões e exclusões de textos para melhor coesão textual.