RESUMO DAS REVISÕES		
Edição	**Data**	**Alteração**
01	05/05/2025	Emissão inicial
02	15/05/2026	Inclusão dos ODS e do Jeito de Cuidar Unimed.

OBJETIVO

Esta política estabelece as diretrizes para a geração, armazenamento, proteção e análise de registros de auditoria (logs) nos sistemas de informação da **Unimed de Tupã**. O objetivo primordial é garantir a rastreabilidade de eventos, apoiar investigações de incidentes e assegurar a conformidade legal, refletindo o compromisso da cooperativa com a transparência e a segurança das informações de seus beneficiários e cooperados.

A gestão de logs na Unimed de Tupã transcende a obrigação técnica, fundamentando-se na **Essência Unimed** e no **Jeito de Cuidar**.

3. APLICAÇÃO

Este documento aplica-se a todos os colaboradores, prestadores de serviço, cooperados e parceiros que utilizam os ativos tecnológicos da **Unimed de Tupã**, abrangendo servidores, bancos de dados, aplicações de gestão de saúde, dispositivos de rede e sistemas de segurança.

4. ALINHAMENTO COM OS OBJETIVOS DE DESENVOLVIMENTO SUSTENTÁVEL (ODS)

Esta política está diretamente vinculada à Agenda 2030 da ONU, reforçando o papel social e institucional da Unimed de Tupã:

- ✓ *ODS 9 (Indústria, Inovação e Infraestrutura):* Ao implementar sistemas de auditoria robustos e resilientes, promovemos uma infraestrutura tecnológica confiável que suporta a inovação e o crescimento sustentável da cooperativa.
- ✓ *ODS 16 (Paz, Justiça e Instituições Eficazes):* A manutenção de logs íntegros assegura a prestação de contas (accountability), combate o uso indevido de informações e fortalece a transparência institucional perante órgãos reguladores e a sociedade.

5. DEFINIÇÕES

- ✓ *Log:* Registro cronológico de eventos ocorridos em um sistema computacional.
- ✓ *Trilha de Auditoria:* Conjunto de logs que permite a reconstrução de uma sequência de eventos.
- ✓ *SIEM (Security Information and Event Management):* Solução tecnológica para agregação e análise centralizada de logs.
- ✓ *NTP (Network Time Protocol):* Protocolo para sincronização de relógios de sistemas.

6. Responsabilidades

- ✓ A atividade de auditoria é de competência da Gestão da Qualidade, gestores de sistemas, área de tecnologia e prestadores de serviço da Unimed de Tupã.
- ✓ A equipe responsável pela auditoria interna deve se reportar ao Diretoria Executiva da Unimed de Tupã.
- ✓ A de TI 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 da empresa Altvia.
- ✓ A Gestão da Qualidade pode obter assessoria de especialistas/consultores externos ou mesmo equipe terceirizada para subsidiar a área quando essa não for suficientemente proficiente.
- ✓ A Gestão da Qualidade 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.
- ✓ É dever dos líderes das áreas cooperar com a da Gestão da Qualidade quanto ao acesso aos ativos de informação, instalações e trânsito de dados.
- ✓ Os membros da Gestão da Qualidade pela auditoria devem ter canal de comunicação permanente com os líderes das áreas para apoiar na atuação corretiva, de forma apropriada e tempestiva, em resposta às recomendações decorrentes dos trabalhos de auditoria.
- ✓ Os eventos de log devem ser gerados, selecionados e armazenados para todos os ativos.
- ✓ A de TI deve selecionar os eventos e os respectivos tempos de guarda, bem como as demais características de uso dos eventos.
- ✓ As exceções deverão ser documentadas.

7. Descrição

a. *Requisitos do plano de registros de auditoria*

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.

Ativos de informação da Unimed de Tupã devem ser configurados de forma a sincronizar data e hora via protocolo *NTP (Network Time Protocol),* onde houver suporte.

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

mal sucedidos aos ativos de informação.

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

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..

Devem ser mapeados os ativos de informação, que por qualquer motivo, não possam apresentar dados detalhados.

Além de eventos em ativos de informação pode registrar eventos de segurança da informação como os a seguir:

Exemplo:

1. Utilização de usuários, perfis e grupos privilegiados;
2. Acoplamento e desacoplamento de dispositivos de hardware, principalmente mídias removíveis;
3. Inicialização, suspensão e reinicialização de serviços;
4. Criação, modificação e exclusão de grupos ou listas de grupos com acessos privilegiados;
5. Atualização das regras da política de senhas de usuários;
6. Criação, acesso e modificação de arquivos de sistemas considerados críticos;
7. Qualquer evento realizado nos ativos de informação de segurança existentes.

Em caso de incidentes de segurança da informação, ou quaisquer outros eventos de segurança, a(o) Gerente de TI deve coletar e preservar todos os registros de eventos citados no na lista de eventos auditáveis definidos (item 7.b.iv) e as mídias de armazenamento dos ativos de informação afetados pelo evento.

Na impossibilidade de seguir o rito padrão de auditoria devido à criticidade do restabelecimento dos serviços, a equipe de TI deverá priorizar a preservação da integridade das evidências. Devem ser coletadas cópias bit-a-bit ou exportações íntegras dos ativos

Exemplo:

a) Logs;
b) Arquivos de sistema operacional;
c) Configurações do sistema operacional; e
d) Demais arquivos e logs que foram necessários para restabelecimento do serviço ou sistema.

A Unimed de Tupã, deve manter a estrutura original de diretórios além dos "metadados" desses arquivos tais como:

Em caso de impossibilidade de preservar as evidências do evento de segurança, o gerente de

TI deve justificar em relatório, a falta destas evidências.

As ações para o restabelecimento do serviço e sistema afetados pelo evento de segurança não devem impossibilitar a coleta, a preservação e disponibilidade das evidências de forma íntegra.

Devem ser promovidas ações para a preservação dos arquivos coletados.

b. Fases da gestão de registros de auditoria

Coleta

i. 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.

ii. Para melhorar o nível de maturidade desta atividade, é importante que a Unimed Tupã 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.

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

iv. A não observância da conformidade das orientações contidas na LGPD e demais regulamentações de privacidade (citadas no subitem iii), pode acarretar prejuízos financeiros e reputacionais, além das sanções administrativas relacionadas no art. 52 da LGPD.

Em caso de incidente de segurança da informação, todo e qualquer material coletado deverão ser lacrados e custodiados pelo agente responsável, e este deve preencher um Termo relacionado ao incidente de segurança.

O material coletado ficará à disposição da autoridade comunicada, a qual orientará quanto a sua destinação.

A geração de log de auditoria deve estar habilitada nos ativos de informação, seguindo as diretrizes do processo de gestão de registros de auditoria da Unimed de Tupã.

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.

Logs devem ser coletados em um ou mais repositórios centrais.

Deve ser assegurado que ativos de informação classificados como críticos estejam registrando logs de auditoria.

Usuários e componentes dos ativos de informação devem ser monitorados continuamente em busca de comportamento anômalo ou suspeito.

Ativos de informação da Unimed de Tupã 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.

A lista de eventos auditáveis definidos deve ser revisada e atualizada periodicamente, pelo menos a cada ano. 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.

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.

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.

c. 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

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.

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 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).

- ✓ O armazenamento de logs deve estar de acordo com o processo de gestão de logs da Unimed de Tupã

- ✓ 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.
- ✓ Registros de auditoria devem ser retidos por pelo menos 3 meses (Logs de sistemas críticos e acesso a dados sensíveis (LGPD) devem ser retidos por no mínimo 6 meses, conforme

recomendações da ISO 27001 para o setor de saúde). Uma vez que o período mínimo de retenção tenha sido atingido, da Unimed de Tupã 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.

✓ 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 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 em nível do sistema.

✓ A capacidade de armazenamento dos logs deve ser constantemente verificada.

✓ Registros de auditoria devem ser correlacionados quando houver mais de um repositório de logs ou coletados de várias fontes de logs.

✓ Cópias de segurança (backups) de arquivos de trilhas de auditoria de log devem ser armazenadas de forma segura, em mídia de difícil alteração.

d. 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.

- ✓ A frequência, escopo e/ou profundidade da revisão, análise e relatório dos registros de auditoria devem ser ajustados para atender às necessidades da Unimed de Tupã com base nas informações recebidas.
- ✓ Análises de logs de auditoria devem ser realizadas pelo menos 1 mês para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial.
- ✓ Processos, procedimentos e medidas técnicas devem ser definidos, implementados e avaliados para reporte de anomalias e falhas do sistema de monitoramento e notificação imediata ao responsável, caso confirmado.
- ✓ 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.
- ✓ 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.
- ✓ 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:

i. Data e hora do evento.
ii. O componente do ativo de informação (por exemplo, componente de software, componente de hardware) onde ocorreu o evento.
iii. Tipo de evento.
iv. Identidade do usuário/sujeito.
v. Resultado (sucesso ou fracasso) do evento.

- ✓ 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 Unimed de Tupã de atingir seus objetivos. As anomalias devem ser analisadas para determinar se representam eventos ou incidentes de segurança.

- ✓ Quando apropriado, logs de auditoria de consultas DNS e URL em ativos de informação devem ser coletados.
- ✓ 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.
- ✓ O comportamento dos ativos de informação deve ser analisado para detectar e mitigar a execução de comandos e scripts que possam indicar ações maliciosas.
- ✓ 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.

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

e. 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.

Recomenda-se a utilização de técnicas de descarte, ou sanitização de dados durante 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 reduzir os custos de armazenamento e gerenciamento de dados.

- ✓ Quando não forem mais necessários para requisitos legais, regulatórios (incluindo federais, estaduais e municipais) ou de negócios da Unimed de Tupã, os dados de logs devem ser removidos dos registros usando um método seguro aprovado.
- ✓ 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.
- ✓ 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 destruídas 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;

✓ 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.
✓ 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 subscrição para não danificar a mídia e ou os dados anteriores não serem expostos de forma desnecessária.

f. RECOMENDAÇÕES TÉCNICAS

✓ Restringir a instalação de aplicativos e softwares. O privilégio de instalação de aplicativos e softwares deve ser restrito a indivíduos autorizados obedecendo aos 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 coletadas 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.

d)

8. Monitoramento

A eficácia desta política será avaliada através de auditorias internas anuais e monitoramento contínuo de alertas gerados pelas ferramentas de segurança. Qualquer tentativa de desativação de logs sem autorização prévia será tratada como incidente grave de segurança.

9. Distribuição de Cópias

Política disponível no Quallix

10. Registros

Relatórios de análise de logs mensais.

Termos de confidencialidade para administradores de sistemas.

Inventário de sistemas críticos com logs ativos.

11. Anexos

Não há

12. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2022**: Segurança da informação, cibersegurança e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 9001:2015**: Sistemas de gestão da qualidade — Requisitos. Rio de Janeiro: ABNT, 2015.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

Aprovação

ANTONIO CARLOS ANDRADE:00190337885

Assinado de forma digital por ANTONIO CARLOS ANDRADE:00190337885
Dados: 2026.05.14 09:03:04 -03'00'

Presidente