Universidade de Brasília

INSTRUÇÃO NORMATIVA DA SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO Nº 001/2024

Dispõe sobre recomendações gerais relacionadas à gestão de registros (*Logs*) para auditoria em ativos críticos de Tecnologia da Informação e Comunicação (TIC) da Universidade de Brasília (UnB).

O SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO DA UNIVERSIDADE DE BRASÍLIA, no uso de suas atribuições ordinárias, considerando a Política de Segurança da Informação e Comunicação (PoSIC) da UnB e Leis e Decretos Federais vigentes que tratam da Gestão de Segurança da Informação e Comunicação (GSIC).

RESOLVE:

Art. 1° Apresentar recomendações essenciais para a gestão de registros (*Logs*) para auditoria em ativos críticos de TIC da UnB, delineando os processos e procedimentos quanto ao ciclo de vida desses registros.

CAPÍTULO I
DAS DEFINIÇÕES

Art. 2° Para efeitos neste documento, foram adotadas as seguintes definições:

ATIVO - Qualquer coisa que tenha valor para a organização.

ATIVOS CRÍTICOS DE TIC - são ativos de TIC (sistemas, aplicações, bases de dados, dispositivos de rede, firewalls, roteadores, dentre outros) que tem um impacto significativo na operação/desempenho da atividade acadêmica e administrativa da UnB, podendo causar prejuízos à produtividade, à segurança e à reputação.

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.

EVENTOS - Quaisquer mudanças 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.

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.

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

LOG DE AUDITORIA – eventos no nível do usuário, informando quem executou a ação, o que e quando. Cada ação registrada em um log contém metadados que indicam o tipo de ação, a data e a hora, a *ID* (identificação) do usuário que executou a ação e atributos adicionais relevantes ao tipo de ação.

LOG DE SISTEMA - eventos no nível do sistema que mostram vários horários de início/término de processo do sistema, travamentos, dentre outros. Eles são nativos dos sistemas e exigem menos configurações para serem ativados NTP *(Network Time Protocol*) – Protocolo de Tempo para Redes.

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.

CAPÍTULO II

PÚBLICO-ALVO, OBJETIVO, ESCOPO E NÃO ESCOPO

SEÇÃO I

PÚBLICO-ALVO

Art. 3° Esta Instrução Normativa se aplica à Secretaria de Tecnologia da Informação (STI), servidores responsáveis pela gestão de ativos críticos de TIC na UnB, bem como às equipes designadas para a prevenção, tratamento e resposta a incidentes cibernéticos dentro da STI.

Parágrafo único: Contudo, a STI poderá orientar as unidades sobre os procedimentos a serem seguidos para ambientes críticos de TIC que não estejam sob a gestão direta da STI. Essa orientação busca assegurar a conformidade com as melhores práticas de segurança e gestão de registros de Logs para auditoria, conforme previsto na Política de Segurança da Informação e Comunicação (PoSIC) da UnB.

SEÇÃO II

OBJETIVO

Art. 4° Recomendar e manter um processo de gestão de registros (*Logs*) que possibilite auditoria em ativos críticos de TIC geridos diretamente pela STI da UnB. Tal processo deve tratar da coleta, armazenamento, uso e exclusão de logs de auditoria, conduzindo revisões periódicas para garantir a conformidade com a segurança e eficiência dos ativos monitorados.

SEÇÃO III
ESCOPO

Art. 5° As recomendações de gestão de registros (*Logs*) se aplicam aos ativos de TIC monitorados e geridos pela STI, incluindo ativos classificados como críticos para a operação e segurança da UnB.

Parágrafo único: Os serviços classificados como críticos serão definidos e listados pela STI em um documento complementar, que estará disponível internamente para consulta. Este documento será atualizado periodicamente, conforme necessário, para refletir quaisquer mudanças nos serviços ou ativos considerados críticos.

SEÇÃO IV
NÃO ESCOPO

Art. 6° Esta Instrução Normativa não se aplica aos ativos de TIC em operação na UnB que não sejam geridos diretamente pela STI ou não classificados como críticos pela STI, exceto nos casos em que as unidades optem voluntariamente por aderir à instrução normativa em questão.

CAPÍTULO III
REGRAS GERAIS

Art. 7° Armazenar registros *(Logs*) no formato padronizado (*Syslog* - RFC 5424) em outro ativo de TIC dedicado, o qual precisa estar em segmento de rede de dados restrito e sem acesso a rede externa.

Art. 8° Manter os ativos críticos de TIC sincronizados quanto a data e hora ao menos com servidor *Network Time Protocol* (NTP) da UnB, o ntp.unb.br.

Art. 9° Preservar todos os registros (*Logs*), as mídias de armazenamento dos ativos críticos de TIC afetados, a estrutura original de diretórios e os metadados de arquivos.

Art. 10 Restaurar operação normal de ativos críticos de TIC afetados por incidentes cibernéticos sem impossibilitar a coleta, a preservação e disponibilidade das evidências de forma integra.

Art. 11 Justificar formalmente a não aplicação de boa prática de armazenamento de logs sobre ativos críticos de TIC.

CAPÍTULO IV

DAS INFORMAÇÕES TÉCNICAS E OPERACIONAIS

Art. 12 Considerar o processo de Gestão de registros (*Logs*) de ativos críticos de TIC em fases de coleta, armazenamento, uso e exclusão, observando para todas as fases a Política de Proteção de Dados Pessoais (LGPD), quando envolver dados pessoais.

Art. 13 Habilitar a nível de *software* ou sistema operacional nos ativos críticos de TIC a geração de registros (*Logs*) de auditoria para eventos significativos, na medida suficiente para estabelecer quais eventos ocorreram, as fontes e os resultados de tais eventos.

SEÇÃO I

COLETA

Art. 14 Assegurar que todos os ativos críticos de TIC produzam registros (*Logs*) na medida necessária e com horário sincronizado para precisão da marcação temporal visando o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

Art. 15 Preservar nos registros (*Logs*) as principais atividades dos usuários, incluindo ao menos tentativas de acesso (sucesso/insucesso), alterações de configurações e permissões, acessos a dados sensíveis, dentre outras informações relevantes.

Art. 16 Preservar em registros (*Logs*) os erros e falhas, os quais podem auxiliar na identificação de problemas de segurança ou de performance, incluindo ao menos falhas de software, de hardware, recursos "estrangulados", dentre outras informações relevantes.

Art. 17 Preservar registros (*Logs*) de sistemas, incluindo ao menos inicializações e desligamentos de sistemas, início/término de processos, travamentos, dentre outros.

Art. 18 Preservar registros (*Logs*) da rede de dados incluindo alterações nas configurações de ativos, fluxos de conexões de entrada e saída, dentre outras informações relevantes, e se necessário, os registros (*Logs*) do provedor de serviços.

Art. 19 Estruturar e manter trilha de auditoria com registro que aponte de forma cronológica e clara as atividades, eventos e procedimentos executados por autor e ações em determinada operação.

Art. 20 Definir quais ativos de informação necessitam de preservação de registros (*Logs*) com eventos mais detalhados e úteis que possam ajudar em uma investigação forense, incluindo:

I . Identificação do evento;

II . origem do evento;

III . identificador de usuário de acesso;

IV . data/hora (*timestamp*) e fuso horário;

V . endereços IPs (*Internet Protocols*);

VI . dentre outras informações relevantes.

Art. 21 Estruturar e manter registros (*Logs*) de auditoria detalhados sobre ativos

críticos de TIC que abriga dados sensíveis, incluindo ao menos:

I . Identificação do evento;

II . origem do evento;

III . carimbo de data/hora (*timestamp*) e fuso horário;

IV . identificação de usuário;

V . endereços IPs de origem e destino.

Art. 22 Manter registros (*Logs*) de acesso a dado pessoal, incluindo ao menos:

I . Identificação do evento (adições, modificações ou exclusões).

II . identificação do usuário;

III . data/hora (*timestamp*) e fuso horário;

IV . titular de dados pessoais que foi acessado.

Art. 23 Implementar trilhas de auditoria automatizadas para reconstruir eventos como:

I . todos os acessos de usuários individuais aos dados sensíveis;

II . todas as ações executadas por usuários com privilégios root ou administrativos;

III . acesso a todas as trilhas de auditoria;

IV . tentativas fracassadas de acesso lógico;

V . usos e alterações dos mecanismos de identificação e autenticação;

VI . criação de novas contas, aumento de privilégios e demais alterações, adições ou exclusões de contas com privilégios root ou administrativos;

VII . inicialização, interrupção ou pausa dos registros de auditoria;

VIII . criação e exclusão de objetos a nível do sistema.

Art. 24 Coletar os registros (*Logs*) de auditoria de consultas *Domain Name System* (*DNS*) e *Uniform Resource Locator* (*URL*) em ativos críticos de TIC.

Art. 25 Coletar registros (*Logs*) de auditoria de linhas de comando (CLI) tais como *PowerShell*, *BASH* e terminais remotos.

SEÇÃO II

ARMAZENAMENTO

Art. 26 Centralizar a retenção de registros (*Logs*) em um ou mais repositórios para aprimoramento do gerenciamento e acompanhar permanentemente a sua capacidade de armazenamento.

Art. 27 Reter de forma segura os registros (*Logs*) de auditoria por pelo menos 1 (um) ano, podendo continuar com a retenção até que seja constatado sua ineficácia para fins administrativos, legais, de auditoria ou outros fins operacionais.

Art. 28 Executar transferência de *logs* (*off-loading*) para armazenamento alternativo de forma que o repositório de destino esteja em uma rede de dados lógica e/ou física diferente e que a transferência ocorra utilizando criptografia para proteger a confidencialidade e integridade dos registros.

Art. 29 Correlacionar registros (*Logs*) de auditoria quando houver mais de um repositório ou quando coletados de várias fontes.

Art. 30 Armazenar de forma segura os backups dos arquivos de trilhas de auditoria de *log*, preferencialmente em mídia de difícil alteração.

SEÇÃO III
USO

Art. 31 Assegurar que os registros (*Logs*) estejam sob controle de acesso e acessíveis quando necessário para análise quanto a comprovação e elucidação de fatos.

Art. 32 Utilizar, preferencialmente, ferramentas automatizadas para monitoramento e análise permanente de registros (*Logs*), que podem identificar padrões estranhos e gerar alertas.

Art. 33 Definir, executar e avaliar processos e medidas técnicas para encaminhamento imediato de anomalias ao responsável pelo ativo crítico de TIC.

Art. 34 Analisar e revisar o relatório dos registros (*Logs*) de auditoria com escopo, frequência e detalhamento suficientes para atender as necessidades da investigação.

Art. 35 Revisar e atualizar regularmente os eventos auditáveis sobre o ativo crítico de TIC, especialmente:

I . tentativas exitosas e fracassadas de *logon*;

II . gerenciamento de contas de usuários;

III . acesso ao serviço de diretório;

IV . exploração de atividade privilegiada;

V . remoção de arquivo de registros (*Logs*) de auditoria.

Art. 36 Identificar e monitorar eventos relacionados a segurança de componentes de infraestrutura computacional subjacente.

Art. 37 Analisar comportamento dos ativos críticos de TIC para descobrir e cessar a execução de comandos/*scripts* que sinalizem possíveis ações maliciosas.

Art. 38 Correlacionar processos de análise, revisão e relatórios de registros (*Logs*) de auditoria, para investigação e resposta a indicações de atividades ilegais, não autorizadas, suspeitas ou incomuns.

SEÇÃO IV
EXCLUSÃO

Art. 39 Realizar a exclusão de dados de registros (*Logs*) seguindo técnicas de descarte de dados baseadas em melhores práticas de segurança da informação, apenas, depois de cumprido os requisitos legais, regulatórios e institucionais.

Art. 40 Estabelecer medidas de proteção para os registros (*Logs*) e controles exclusivos para registro das ações dos administradores e operadores dos ativos críticos de TIC, de forma que não tenham permissão de exclusão ou desativação de registros de suas próprias ações.

Art. 41 Assegurar que a exclusão de dados de logs em mídias físicas/digitais e em impressos ocorra em método seguro de modo a não possibilitar a sua recuperação.

CAPÍTULO V
DAS RESPONSABILIDADES

Art. 42 Os responsáveis pelos ativos críticos de TIC devem considerar a aplicação proativa ao disposto nesta norma.

SEÇÃO I
DA STI

Art. 43 A STI é responsável por estabelecer processos de gestão de registros (*Logs*) e Auditoria, designando competências ordinárias à equipe responsável pelo tema de segurança da informação na STI, à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) da UnB e aos gestores/administradores de ativos críticos de TIC sob sua gestão. Parágrafo único. A STI, conforme necessário, orientará outras unidades da UnB sobre procedimentos recomendados para ativos críticos de TIC não diretamente geridos por ela, garantindo a conformidade com as diretrizes de segurança e gestão de *logs*.

Art. 44 Desenvolver e manter competência técnica e administrativa no gerenciamento de registros (*Logs*), atuando com autonomia, neutralidade, zelo, seriedade e ética profissional.

Art. 45 Obter consultoria de profissional(ais) externo(s) para auxiliar no escopo técnico, quando necessário.

SEÇÃO II
GESTORES/ADMINISTRADORES DE ATIVOS CRÍTICOS DE TIC

Art. 46 Zelar por estas recomendações e outras complementares à PoSIC.

Art. 47 Aplicar sobre ativos críticos de TIC sob sua responsabilidade técnica a gestão de registros (*Logs*).

Art. 48 Colaborar ativamente em demandas relacionadas a gestão de registros (*Logs*) e na atividade de auditoria;

CAPÍTULO VI
ATUALIZAÇÕES E REVISÕES

Art. 49 Alterações de processos internos, tecnologia e recursos providos pela STI podem ocasionar em atualizações deste documento.

Art. 50 Casos omissos a esta norma que consequentemente gera a necessidade de sua atualização.

Art. 51 Surgimento e/ou atualizações de normativos, leis e regulamentações vigentes.

Art. 52 Este documento será revisado a qualquer momento a critério da STI.

Art. 53 Esta instrução Normativa entra em vigor na data de sua publicação.

Brasília, 07 de novembro de 2024.

Documento assinado eletronicamente por **Jacir Luiz Bordim**, **Secretário(a) de Tecnologia da Informação**, em 07/11/2024, às 18:30, conforme horário oficial de Brasília, com fundamento na Instrução da Reitoria 0003/2016 da Universidade de Brasília.

A autenticidade deste documento pode ser conferida no site http://sei.unb.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **11990166** e o código CRC **9AD4F418**.

Referência: Processo nº 23106.110020/2024-91 SEI nº 11990166