Diário Oficial
Imprensa Nacional
REPÚBLICA FEDERATIVA DO BRASIL
BRASÍLIA - DF
Nº 118 - DOU – 23/06/2023 - Seção 1 – p.53

MINISTÉRIO DA EDUCAÇÃO
FUNDAÇÃO COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR

PORTARIA CAPES Nº 116, DE 20 DE JUNHO DE 2023

Institui a norma de Registro de Eventos (logs) do Ambiente Computacional da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES

A PRESIDENTE DA COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR - CAPES, no uso das atribuições que lhe foram conferidas pelo art. 33, inciso IX do Estatuto aprovado pelo Decreto nº 11.238, de 18 de outubro de 2022, com fundamento no art. 12, inciso VII, § 2º da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 e suas alterações; na Norma Complementar nº 21/IN01/DSIC/GSIPR, de 10 de outubro 2014; e na Política de Segurança da Informação e Comunicações da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES , resolve:

Art. 1º Aprovar a norma de Registros de Eventos (logs) do Ambiente Computacional da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES.

CAPÍTULO I

DOS OBJETIVOS

Art. 2º Esta portaria define as diretrizes a serem adotadas no tratamento dos registros de eventos (logs) do ambiente computacional da CAPES.

Art. 3º As ações que ocorrem no ambiente computacional devem ser registradas em eventos (logs) de forma a permitir a rastreabilidade inequívoca das atividades, sejam para fins de monitoramento, auditoria ou investigação de incidentes de segurança. Os ativos de Tecnologia da Informação e Comunicação - TIC devem ser configurados para registrar tais ações, como:

I - autenticação e autorização com sucesso ou não;

II - registros, consultas e modificações em páginas, dados, grupos, políticas e entre outros;

III - inicialização, suspensão e reinicialização de serviços ou programas;

IV - acoplamento e desacoplamento de dispositivos;

V - comandos e interações nos sistemas operacionais; e

VI - dados do desempenho do ativo.

CAPÍTULO II

SINCRONISMO DO TEMPO

Art. 4º Para garantir o exato momento do evento, os ativos de TIC devem estar configurados com o "Serviço de Sincronização de Tempo" (NTP - Network Time Protocol) central do órgão.

§ 1º O horário dos ativos deve ser monitorado de forma automatizada com objetivo de garantir a correta sincronização do tempo.

§ 2º O servidor de tempo central do órgão deve utilizar no mínimo duas fontes confiáveis, sendo uma delas o NTP.br.

CAPÍTULO III

REGISTRO, ARMAZENAMENTO E COLETA DOS LOGS

Art. 5º Os dados mínimos necessários no registro de um log, quando aplicável, devem ser:

I - data/hora com timezone;

II -endereço de origem com IP e/ou hostname do cliente, mesmo quando atrás de outro ativo (proxy);

III -endereço de destino com IP e/ou hostname;

IV - nome do usuário (login);

V - tipo de ação executada (consulta, inclusão, alteração, exclusão); e

VI - protocolo e serviço (porta) utilizados;

Art. 6º O prazo de armazenamento dos logs, do ambiente de produção, deverá ocorrer de acordo com o "ANEXO A - PRAZOS DE RETENÇÃO DOS LOGS - AMBIENTE PRODUÇÃO", a depender da criticidade do ativo e do tipo de log gerado, no qual este último poderá ser:

I - tipo A: Auditoria e Acesso - registro da ação que indica "quando", "quem" e "o que" foi feito no ativo;

II - tipo B: Sistema Operacional e Comandos - eventos gerados automaticamente pelo sistema operacional e dos serviços nele instalados e do histórico dos comandos utilizados em um ativo como servidores de rede, switches, roteadores, firewalls; e

III - tipo C: Debug: tipos de eventos utilizados para investigação de problemas e resolução de erros: rastreamento de pilha (stack trace), mensagens de erros (error messages), captura de tráfego de rede (network dumps).

Parágrafo único: O prazo de armazenamento para os demais ambientes (desenvolvimento, homologação, teste - DHT) encontra-se no "ANEXO B - PRAZOS DE RETENÇÃO DOS LOGS - AMBIENTE DHT".

Art. 7º O local de armazenamento dos registros de eventos e/ou trilhas de auditoria (logs) será designado por fases, sendo elas:

I - fase Corrente: utilizados para consulta rápida dos eventos, os logs podem ser armazenados em:

a) local: no próprio servidor ou em local mapeado em um storage;

b) Centralizador de Logs: serviço de rede dedicado ao armazenamento organizado dos eventos, como: LMS (Log Management System) ou SIEM (Security Information and Event Management); e

c) base de Dados: gravação dos eventos em tabelas de bancos de dados (SGBDs).

II - fase Intermediária: - utilizados, além do backup, mas também para economia de recursos, podendo ser armazenados em:

a) fita: armazenamento de dados em fita magnética; e

b) outros: uso de serviços externos como provedores de nuvem.

Art. 8º Os logs "Tipo A" e "Tipo B", das aplicações consideradas críticas, devem ser armazenados em um "Centralizador de Logs","Banco de Dados" ou "Local" desde que este último esteja utilizando um storage externo ao ativo, para que seja possível visualizar os logs no caso de incidente com o ativo.

Art. 9º O método de coleta do log será padronizado, considerando:

I - a nomenclatura do nome do arquivo de log - deverá seguir o padrão "<aplicacao>.capes.capes.gov.br[-XXX].log", onde "[-XXX]" é opcional para especificar algum tipo de log. Exemplo: "www.capes.gov.br-acesso.log" ou simplesmente "www.capes.gov.br.log";

II - no envio para "Centralizador de Logs" / "Banco de Dados", recomenda-se que o envio seja feito utilizando-se criptografia na comunicação; e

III - o envio para "Centralizador de Logs" deverá ser feito por meio de protocolos homologados pela CGII, como: GELF, SYSLOG e outros.

Parágrafo único: A CGII publicará os procedimentos operacionais necessários para o envio de logs.

Art. 10. Quando aplicável, para conferir mais eficiência no tratamento dos logs armazenados localmente, deve-se:

I - realizar rotacionamento diário;

II - compactar arquivos indicando no nome do arquivo a data no formato "ano", "mês" e "dia", exemplo: "<aplicação>[<.ambiente>].capes.gov.br.log-AAAAMMDD.gz"; e

III - possibilitar a geração de arquivo com hash dos arquivos armazenados.

Art. 11. A estrutura padrão do conteúdo dos logs serão homologados e padronizados pela CGII e divulgado internamente.

CAPÍTULO IV

ACESSO E MONITORAMENTO DOS LOGS

Art. 12. As equipes terão acessos aos logs do "Tipo C - Debug"," de suas respectivas aplicações.

Parágrafo único: A equipe de infraestrutura de TI terá acesso aos logs do "Tipo C-Debug" de todas as aplicações.

Art. 13. Os logs do "Tipo B - Sistema Operacional" serão acessados pela equipe de infraestrutura de TIC.

Art. 14. Devido a sensibilidade dos logs do "Tipo A - Auditoria e Acesso", observado a Política de Segurança, o acesso será permitido mediante autorização do coordenador CGII ou do Gestor de Segurança da Informação.

Art. 15. O compartilhamento dos dados, interna ou externamente, somente poderá ocorrer mediante autorização do coordenador diretamente relacionado, sendo recomendado a anonimização de dados sensíveis e pessoais, como endereço IP e login do usuário, entre outras.

Art. 16. As equipes são responsáveis pelo monitoramento e investigação dos problemas identificados em suas respectivas aplicações, podendo solicitar o auxílio da equipe de infraestrutura.

Parágrafo único: Incidentes de segurança identificados ou suspeitos, devem ser notificados imediatamente à Equipe de Tratamento de Incidentes.

Art. 17. Esta Portaria entra em vigor em 1º de julho de 2023.

MERCEDES MARIA DA CUNHA BUSTAMANTE

ANEXO A

PRAZOS DE RETENÇÃO DOS LOGS - AMBIENTE DE PRODUÇÃO

Criticidade do Ativo	Tipo de Log	Retenção (Prazo de Guarda)		Retenção Total* (Corrente e Intermediária)	Destinação Final24
		Fase Corrente* (***online***)	Fase Intermediária* (off line)		
Crítico	Tipo A	2 anos	5 anos	7 anos	Eliminação
Não Crítico	Tipo A	1 ano	4 anos	5 anos	Eliminação
- (qualquer criticidade)	Tipo B	1 ano	1 ano	2 anos	Eliminação
- (qualquer criticidade)	Tipo C	1 mês	-	1 mês	Eliminação
A "Retenção Total" deve ser atendida, mas o prazo da "Fase Corrente" e da "Fase Intermediária" poderá ser ajustada conforme necessidade.					

ANEXO B - PRAZOS DE RETENÇÃO DOS LOGS - AMBIENTE DHT

Criticidade do Ativo	Tipo de Log	Retenção (Prazo de Guarda)		Retenção Total* (Corrente e Intermediária)	Destinação Final
		Fase Corrente (***online***)	Fase Intermediária (off line)		
- (qualquer	Tipo A	3 meses	- 3 meses	Eliminação	

criticidade)					
- (qualquer criticidade)	Tipo B	3 meses	-	3 meses	Eliminação
- (qualquer criticidade)	Tipo C	7 dias	-	7 dias	Eliminação