INSTRUÇÃO NORMATIVA Nº 301, DE 09 DE JULHO DE 2024

Dispõe sobre o processo de gestão e monitoramento de registros de atividades (logs) dos sistemas e recursos informatizados do Supremo Tribunal Federal.

***O DIRETOR-GERAL DA SECRETARIA DO SUPREMO TRIBUNAL FEDERAL**, no uso das atribuições que lhe confere o art. 41, inciso X, alínea b, do Regulamento da Secretaria de 2024, e tendo em vista o que consta do Processo Administrativo eletrônico 003014/2023;*

***CONSIDERANDO** a Lei 12.965/2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;*

***CONSIDERANDO** o direito fundamental à autodeterminação informativa (art. 5º, LXXIX, da Constituição Federal) e a entrada em vigor da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);*

***CONSIDERANDO** que a LGPD estabelece as condições sob as quais os dados pessoais podem ser tratados, define um conjunto de direitos para os titulares dos dados e impõe obrigações específicas aos controladores dos dados;*

***CONSIDERANDO** a Resolução 759/2021, que institui a Política de Privacidade e de Proteção de Dados;*

***CONSIDERANDO** a Resolução 773/2022, que institui a Política de Segurança da Informação do STF;*

***R E S O L V E**:*

Art. 1º Instituir o Processo de Gestão e Monitoramento de Registro de Atividades dos sistemas e recursos informatizados do Supremo Tribunal Federal (PGMRA/STF).

CAPÍTULO I

DOS CONCEITOS E DEFINIÇÕES

Art. 2º Para os efeitos desta instrução normativa, aplica-se o glossário de termos de segurança da informação definido e publicado no Repositório Digital do STF (https://bibliotecadigital.stf.jus.br/xmlui/).

CAPÍTULO II

DOS PRINCÍPIOS

Art. 3º O PGMRA/STF se alinha às estratégias do STF, de sua Política de Segurança da Informação e de sua Política de Privacidade e de Proteção de Dados, tendo como premissa possibilitar:

I – a identificação detalhada das causas de eventos ocorridos em ativos de informação do STF e as respostas às respectivas causas;

II – a responsabilização da autoria de eventos;

III – a verificação da origem dos eventos.

CAPÍTULO III

DO ESCOPO

Art. 4º São objetivos do PGMRA/STF:

I – estabelecer as diretrizes, responsabilidades e competências para a Gestão e Monitoramento de Registros de Atividades dos sistemas e ativos do Tribunal;

II – manter uma base confiável e consolidada para auditorias e para o tratamento de incidentes de segurança da informação.

Art. 5º O PGMRA/STF se aplica a todas as autoridades, servidores e colaboradores do STF que usam ou tenham acesso aos ativos de informação e de processamento no âmbito do Tribunal.

§ 1º Todos são responsáveis pela segurança da informação, devendo, para tanto, conhecer e seguir a presente IN.

§ 2º A Administração do Tribunal promoverá programas de conscientização sobre o uso de ativos de informação e processamento.

CAPÍTULO IV

DA COLETA DE REGISTROS DE ATIVIDADES EM SISTEMAS OPERACIONAIS

Art. 6º Os proprietários dos ativos são responsáveis por garantir a habilitação e validação da conformidade dessa norma com os registros de atividades realizados pelos ativos.

Art. 7º Os registros de atividades devem conter informações mínimas e relevantes, especialmente:

I – natureza do evento a ser registrado, tais como:

a) tentativas de autenticação, bem-sucedidas ou não;

b) trocas de senhas;

c) alteração, modificação ou eliminação de registros de banco de dados;

d) acesso a registros de banco de dados classificados;

e) registros de acesso a sites de internet;

f) uso de funcionalidade relevante de aplicações, tais como assinatura digital em processo, elaboração e modificações de minutas de decisão, registros de andamento processual, entre outros;

g) estabelecimento de conexão;

II – identificação inequívoca do usuário que acessou o recurso;

III – identificação dos usuários de origem e destino do evento, quando for o caso;

IV – data e hora, no padrão internacional ISO-8601, utilizando o formato "YYYY-MM-DDThh:mm:ss,SSSZ", onde YYYY representa o ano, MM representa o número do mês, DD representa o número do dia, hh representa a hora em 24 horas, mm representa os minutos, ss representa os segundos, SSS representa os milissegundos, e Z o fuso horário UTC, que utiliza a Hora Universal Coordenada;

V – endereço de IP de origem, endereço IP de destino, porta de origem, porta de destino, protocolo e quantidade de dados trafegados, quando for o caso;

VI – recurso acessado e tipo de acesso.

Parágrafo único. Os proprietários dos ativos devem instituir rotinas periódicas que revisem os logs para identificar eventos anormais.

Art. 8º Os registros de atividades serão armazenados pelo período de 1 (um) ano, e devem ser objeto de cópias de segurança, nos termos de normativo específico.

CAPÍTULO V

MONITORAMENTO DOS EVENTOS DE ACESSO OU USO

Art. 9º Os ativos de processamento em produção devem ser configurados de forma a gerar registros de atividades relevantes que afetem a segurança da informação ou a proteção de dados pessoais, incluindo:

I – registros de conexões com IP de origem, IP de destino, porta de origem, porta de destino, protocolo e quantidade de dados trafegados;

II – acesso remoto à rede corporativa;

III – autenticação, tanto a bem-sucedida quanto a malsucedida;

IV – criação, alteração e remoção de usuários, perfis e grupos privilegiados;

V – uso de privilégios;

VI – troca de senhas;

VII – modificação de política de senhas;

VIII – acesso ou modificação de arquivos, serviços e sistemas de informação considerados críticos;

IX – alteração na configuração de sistemas operacionais, serviços e sistemas de informação;

X – inicialização, suspensão e reinicialização de serviços;

XI – uso de aplicativos e utilitários no sistema operacional;

XII – ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção e prevenção de intrusos;

XIII – acoplamento e desacoplamento de dispositivos de hardware, com especial atenção a mídias removíveis;

XIV – acesso e alteração nos registros de logs;

XV – uso da rede sem fio.

Art. 10. O monitoramento deve ser realizado com a utilização de ferramentas automatizadas que gerem alertas imediatos de eventos críticos e permitam correlação e análises dos registros de eventos gerados.

Parágrafo único. A STI deve, periodicamente, ajustar as configurações de ferramentas para correção e análise de registros de atividades de forma a diminuir o ruído proveniente de eventos não importantes.

Art. 11. Os usuários deverão assinar termo de compromisso quanto ao cumprimento desta instrução normativa, e nele tomar ciência de que os ativos de informação estão sujeitos a monitoramento e auditoria.

CAPÍTULO VI

DA SINCRONIZAÇÃO DE RELÓGIOS

Art. 12. Os registros de atividades devem ser registrados no Tempo Universal Coordenado (TUC ou UTC).

Art. 13. Os relógios dos ativos de informação devem utilizar, ao menos, três fontes de horários sincronizados.

Parágrafo único. A sincronização deve ser feita, preferencialmente, utilizando o protocolo NTS.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 14. Os casos omissos serão resolvidos pelo Comitê Executivo de TI.

Parágrafo único. Quando o caso omisso envolver ativos de informação que contenham dados pessoais, o Comitê Executivo de TI resolverá em conjunto com o Comitê Executivo de Proteção de Dados (CEPD).

Art. 15. Esta instrução normativa entra em vigor na data de sua publicação, e sua implementação será feita no prazo de 12 (doze) meses a contar dessa data.

EDUARDO S. TOLEDO

Publicado no DJE/STF em 10/7/2024.