Poder Judiciário
Conselho Nacional de Justiça

PORTARIA PRESIDÊNCIA N° 186 DE 14 DE JUNHO DE 2024.

Regulamenta o tratamento administrativo de incidentes por acesso indevido a sistemas gerenciados pelo Conselho Nacional de Justiça.

O **PRESIDENTE DO CONSELHO NACIONAL DE JUSTIÇA (CNJ)**, no uso de suas atribuições legais e regimentais, e tendo em vista o contido no processo SEI nº 06353/2024,

CONSIDERANDO a necessidade de criar procedimento administrativo de cancelamento e apuração de eventuais ordens judiciais ilegítimas em sistemas eletrônicos gerenciados pelo Conselho Nacional de Justiça;

CONSIDERANDO o disposto no art. 11, I, II e XI, e 23, VII, da Resolução CNJ nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

RESOLVE:

Art. 1º Regulamentar o tratamento administrativo de incidentes por acesso indevido a sistemas gerenciados pelo Conselho Nacional de Justiça.

Art. 2º Caso constatado, por magistrado(a) ou servidor(a) de qualquer tribunal brasileiro, em sistemas eletrônicos gerenciados pelo CNJ, indício de ordem judicial ilegítima decorrente de uso indevido de credenciais (*login*, senha ou fatores de autenticação) ou outro meio de acesso, deverá este informar o ocorrido, de forma urgente, de preferência via *e-mail* funcional, à Divisão de Segurança da Informação (DISI) do CNJ fornecendo, sempre que possível e de forma cooperativa:

I – uma declaração escrita e assinada de próprio punho contendo seu nome completo e Cadastro de Pessoas Físicas (CPF), individualizando o sistema e o ato reputado como fraudulento, bem como a data em que a ação teria sido praticada e demais informações que auxiliem na sua perfeita identificação, inclusive captura de tela;

II – a informação se utiliza frequentemente aquele sistema e, em caso negativo, a data próxima da qual teria feito uso do sistema pela última vez;

III – caso utilize frequentemente o sistema, a forma pela qual o acessa, se via *login* e senha, certificado digital ou por outro meio, como a plataforma Gov.BR;

IV – seu *login* de acesso ao sistema, bem como seu *e-mail* funcional no respectivo tribunal;

V – quais sistemas eletrônicos gerenciados pelo CNJ utiliza habitualmente; e

VI – se delega ou autoriza o acesso a sistemas a servidor(a) do respectivo tribunal e, em caso positivo, qual o nome completo, CPF e *login* de acesso do(a) servidor(a).

Parágrafo único. Tão logo possível, deverá o(a) usuário(a) providenciar a troca de sua senha de acesso ao sistema e a habilitação do segundo fator de autenticação, caso ainda não tenha sido realizado.

Art. 3º De posse dos dados do(a) usuário(a) afetado e da respectiva ação ilegítima, a Divisão de Segurança da Informação (DISI/CNJ) deverá proceder a abertura de processo no Sistema Eletrônico de Informação (SEI), ou juntada da notícia do incidente em outro já aberto e que apure outros incidentes em face de mesmo(a) usuário(a), e a sucessiva comunicação ao(à) respectivo(a) Gestor(a) do sistema no CNJ.

Parágrafo único. Havendo incidentes de segurança em face de outros(as) usuários(as) do mesmo tribunal, os processos deverão ser apensados no SEI.

Art. 4º Verificada a situação e confirmada a ação ilegítima, o(a) Gestor(a) do sistema no CNJ deverá determinar o imediato cancelamento administrativo da ação no sistema, documentando por despacho no processo SEI com cópias das telas (do ato ilegítimo e do cancelamento), bem como deverá dar ciência do cancelamento ao(à) magistrado(a) ou servidor(a) e, se for o caso, às demais instituições ou órgãos afetados pelo fato.

§ 1º A depender da extensão do incidente ou de suas circunstâncias, poderá o(a) Gestor(a) do sistema no CNJ determinar o imediato bloqueio cautelar de acesso do(a) usuário(a) a todos os sistemas gerenciados pelo CNJ, incluindo o encerramento de eventuais sessões ativas, a remoção de credenciais armazenadas e o *reset* da senha utilizada, comunicando-o(a) da forma possível, até que garantido o seu restabelecimento seguro.

§ 2º Nos casos de bloqueio, somente deverá ser restabelecido o acesso ao(à) usuário(a) após recebimento de informação da área de segurança cibernética do tribunal de origem garantindo que os dispositivos (computadores e aparelhos celulares) utilizados pelo(a) magistrado(a) ou servidor(a) estão seguros e livres de malware.

Art. 5º A DISI/CNJ deverá prosseguir na apuração do incidente e verificar ao menos:

I – a forma de acesso ao sistema quando da prática da ação ilegítima;

II – o endereço IP e a data/hora quando da prática da ação ilegítima;

III – um extrato das ações praticadas com o referido *login* no sistema em que foi verificada a ação ilegítima que abranja, desde a data atual, até a data do último acesso legítimo informada pelo(a) usuário(a) ou, em caso de acesso habitual, da data atual até ao menos 3 (três) meses antes da data do acesso ilegítimo;

IV – um extrato das ações praticadas com o referido *login* em quaisquer outros sistemas gerenciados pelo CNJ que também possam ter sofrido acessos pelo mesmo(a) usuário(a), que abranja o período desde a data atual até ao menos 3 (três) meses antes da data do acesso ilegítimo.

§ 1º A DISI/CNJ poderá solicitar informações complementares a outras unidades do CNJ, ao(à) usuário(a) ou ao tribunal, incluindo a emissão de Relatório de Incidente de Segurança pela Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) do tribunal correspondente.

§ 2º Os dados levantados deverão ser apensados no processo SEI correspondente ou armazenados em repositório de arquivos do CNJ.

§ 3º A DISI/CNJ poderá encaminhar ao(à) usuário(a) ou ao tribunal de origem, orientações de medidas complementares de segurança, sem prejuízo de ações semelhantes pela diretoria do DTI do CNJ ou pelo(a) gestor(a) do sistema no CNJ.

Art. 6º Concluída a apuração mínima, deverá a DISI/CNJ dar ciência dos dados apurados ao(à) Gestor(a) do sistema no CNJ que, por sua vez, constatados indícios de ato ilícito, deverá providenciar a comunicação do fato à Polícia Federal, por um dos seguintes meios:

I – via ofício à unidade da Polícia Federal que já acompanha fatos anteriores relacionados ao(à) mesmo(a) usuário(a) ou sistema, quando então deverá instruir o ofício com o número do inquérito policial a que se refere; ou

II – encaminhar os autos à Secretaria-Geral quando se tratar de fato cuja apuração policial ainda não seja de seu conhecimento, quando então deverá a(o) Secretária(o)-Geral encaminhar ofício à Polícia Federal solicitando a abertura de inquérito policial.

Parágrafo único. O cancelamento administrativo de novas ações ilegítimas, desconhecidas pelo(a) usuário(a), deverá ser realizada pelo respectivo(a) Gestor(a) do Sistema no CNJ após a verificação e confirmação da ação ilegítima pelo(a) usuário(a) ou tribunal de origem.

Art. 7º Esta Portaria entra em vigor na data de sua publicação.

Ministro **Luís Roberto Barroso**

Documento assinado eletronicamente por **Luís Roberto Barroso**, **PRESIDENTE**, em 14/06/2024, às 18:32, conforme art. 1º, §2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no portal do CNJ informando o código verificador **1866783** e o código CRC **471DFAE9**.