REPÚBLICA FEDERATIVA DO BRASIL
PODER JUDICIÁRIO
Seção Judiciária de Pernambuco

Diário Eletrônico Administrativo SJPE

Nº 55.0/2022 Recife - PE, Disponibilização: Terça-feira, 22 Março 2022

Direção Geral do Foro

Portaria

PORTARIA DA DIREÇÃO DO FORO

Nº55/2022

Institui a Norma de Controle de Acesso Lógico e Físico aos Ativos de Informação da Justiça Federal em Pernambuco.

O MM. Juiz Federal Diretor do Foro, no uso de suas atribuições legais e regimentais, e

CONSIDERANDO a Resolução CJF n°6, de 07 de abril de 2008, que dispõe sobre a implantação da Política de Segurança da Informação e a utilização dos ativos de informática no âmbito do Conselho e da Justiça Federal de primeiro e segundo graus, alterada pela Resolução CJF n° 687, de 15 de dezembro 2020;

CONSIDERANDO as Normas Técnicas NBR ISO/IEC 27001:2013, que trata de Sistemas de Gestão da Segurança da Informação, e NBR ISO/IEC 27005:2019, que trata da Gestão de Riscos de Segurança da Informação;

CONSIDERANDO a Lei 12.527/2011 - Lei de Acesso à Informação;

CONSIDERANDO a Lei 12.965/2014 - Marco Civil da *Internet*;

CONSIDERANDO a Lei 13.709/2018 - Lei Geral de Proteção de Dados Pessoais;

CONSIDERANDO a Portaria CNJ 242/2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário;

CONSIDERANDO a Portaria da Direção do Foro nº 54/2022, que estabeleceu a Comissão Local de Segurança da Informação da Justiça Federal em Pernambuco,

RESOLVE:

Art. 1º Instituir a Norma de Controle de Acesso Lógico e Físico aos Ativos de Informação da Justiça Federal em Pernambuco.

Parágrafo único. Esta norma norteará a implementação de medidas para regular a segurança no acesso lógico e físico de pessoas aos recursos de processamento, armazenamento e comutação de dados corporativos de Tecnologia da Informação (TI) da Justiça Federal em Pernambuco e suas subseções de forma a minimizarem os riscos à segurança das informações corporativas, para usuários internos e externos.

TERMOS E DEFINIÇÕES

Art. 2º Para efeitos desta resolução, aplicam-se as seguintes definições:

a) Agente público: magistrados, servidores, estagiários e prestadores de serviço que estejam exercendo atividades na Justiça Federal em Pernambuco.

b) Área de Tecnologia da Informação: unidade responsável pela Tecnologia da Informação, Núcleo de Tecnologia da Informação (NTI)

c) Acesso lógico: acesso por meio de tecnologia da informação - TI aos sistemas, softwares e aplicativos da instituição;

d) Acesso físico: acesso de pessoas aos ativos de informação. O sistema de controle de acesso físico é composto de mecanismos de controle e procedimentos que garantam a segurança desses ativos.

e) *Backup*: cópia de segurança dos dados.

f) Conta de acesso: identificação do usuário, com senha associada, para acesso aos recursos de TI

g) *Firewall*: sistema de rede que monitora e aplica regras de segurança a fluxo de dados.

h) Gestor de Sistema: agente público ou comissão oficialmente designados para a gestão de determinado sistema de informação.

i) LAN: sigla em inglês para *Local Area Network* ou rede local.

j) *Link* de trânsito: nome dado à conexão da rede privada com a rede pública.

k) Unidade Institucional: unidade de lotação do agente público.

l) Usuário: pessoa física ou jurídica que opera algum sistema informatizado da Justiça Federal.

m) VPN: do inglês *Virtual Private Network*, ferramenta que permite o acesso a redes privadas por meio de rede pública.

Parágrafo único. Aplicam-se a esta resolução os termos e definições constantes da Política de Segurança da Justiça Federal.

CADASTRAMENTO DE USUÁRIOS

Art. 3º A criação de contas de acesso à rede interna da Justiça Federal em Pernambuco se vinculará à data de entrada em exercício do usuário interno ou do colaborador.

§ 1º A conta de acesso será de uso pessoal e intransferível e em nenhuma hipótese poderá ser compartilhada.

§ 2º Para os sistemas que não oferecem o gerenciamento centralizado de usuário e senha, o gestor da unidade deverá encaminhar eletronicamente, no sistema apropriado, pedido formal ao gestor do respectivo sistema, que manterá registro de todos os pedidos de inclusão, exclusão e alteração de perfil de usuário.

§ 3º A conta de acesso no perfil Administrador somente será fornecida aos usuários cadastrados para execução de tarefas específicas na administração de ativos de informação e não deverá ser compartilhada

Art. 4° A conta de acesso à rede interna e aos serviços de TI será bloqueada quando do desligamento do usuário interno ou do colaborador.

§ 1º Considera-se desligamento a exoneração, demissão, aposentadoria, falecimento ou qualquer outro tipo de afastamento definitivo do usuário.

§ 2° É responsabilidade do gestor da unidade solicitar o bloqueio da conta de acesso quando do desligamento.

POLÍTICA DE SENHAS

Art. 5º A identificação de usuários que operam os sistemas deve ser feita mediante a autenticação usuário-senha, preferencialmente com duplo fator de autenticação ou certificado digital.

Parágrafo único. Essa identificação está dispensada para consulta a sistemas públicos da Justiça Federal em Pernambuco, como o portal eletrônico, contudo a área de Tecnologia da Informação deverá manter registros para auditoria de acesso.

Art. 6º A senha cadastrada é pessoal, intransferível e confidencial.

Art. 7º As regras de formação e de duração das senhas serão definidas pela Comissão Local de Segurança da Informação e terão ampla divulgação.

ACESSO À REDE

Art. 8º Apenas poderão ser conectados às redes cabeadas da Justiça Federal em Pernambuco dispositivos previamente autorizados pela respectiva área de Tecnologia da Informação.

§ 1º Exceções devem ser comunicadas à Direção do Foro, justificando a necessidade e o prazo de utilização.

§ 2º As exceções autorizadas deverão obrigatoriamente adotar os padrões definidos pela Política de Segurança da Justiça Federal em Pernambuco, sendo o proprietário do equipamento responsável pelo licenciamento dos produtos nele instalados, além da manutenção e suporte aos sistemas não homologados pela área de Tecnologia da Informação, sendo que a Justiça Federal em Pernambuco não fornecerá licenças para funcionamento de microcomputadores particulares.

Art. 9º Microcomputadores e/ou dispositivos portáteis não pertencentes à Justiça Federal em Pernambuco só poderão acessar a rede sem fio específica para esse fim mediante prévio cadastramento e autorização.

Parágrafo único. O usuário, antes de acessar a "rede visitante", deverá se identificar e concordar com o termo de uso da rede sem fio.

Art. 10º A área de Tecnologia da Informação poderá desconectar das redes cabeada e sem fio qualquer dispositivo que constitua ameaça à segurança da informação.

Art. 11. A área de Tecnologia da Informação poderá utilizar equipamentos e serviços de segurança para inspecionar qualquer ambiente de rede, cabeada ou sem fio, para identificar invasões, ameaças e falhas.

Art. 12. A conexão de outras instituições à rede corporativa deverá ser executada pelo *link* de trânsito da instituição, ficando vedada a conexão do tipo ponto a ponto ou â€œLAN" *to* "LAN".

Parágrafo único. Caso seja necessário conexão privada, poderá ser feita conexão do tipo VPN, sendo as configurações de protocolo definidas pela área de Tecnologia da Informação.

Art. 13. A área de Tecnologia da Informação poderá utilizar protocolos e serviços para privilegiar tráfego de rede, bem como restringir ou bloquear fluxos de rede, garantindo a banda necessária para execução de sistemas considerados essenciais pela Administração.

Parágrafo único. Instalação e ou manutenção de serviços, periféricos, dispositivos e outros equipamentos, que utilizem banda de dados, necessitam a autorização da área de Tecnologia da Informação para implementação.

Art. 14. Todo o tráfego da rede corporativa, cabeada ou sem fio, será inspecionado por serviços de *firewall* e equipamentos de segurança de redes, visando proteger a rede, combater ameaças cibernéticas ou fuga de dados sensíveis à instituição.

Parágrafo único. A área de Tecnologia da Informação poderá aplicar políticas de bloqueio aos fluxos de dados para garantir a segurança do ambiente.

Art. 15. A área de Tecnologia da Informação poderá aplicar bloqueios em portas físicas de equipamentos de rede, para garantir que apenas um equipamento esteja conectado.

ACESSO A PORTAIS DA *INTERNET*

Art. 16. Todo acesso à *internet* deverá ser identificado por usuário.

§ 1º Os rastros de acesso deverão, no mínimo, identificar usuários, endereços IP (protocolo de *internet*), URL (endereço virtual do local do arquivo, sítio etc.) acessada, data e hora.

§ 2º A área de Tecnologia da Informação deverá reter os rastros de acesso pelo prazo mínimo de 5 anos.

Art. 17. É proibido o acesso a sítios que contenham materiais (1) pornográficos, obscenos ou correlatos, (2) ofensivos, preconceituosos ou de discriminação étnica, sexual ou religiosa; ou que tratem de (3) ferramentas para invasão e evasão de sistemas, (4) anonimização de acesso e (5) apologia ou incitação a crimes.

Parágrafo único. A área de Tecnologia da Informação poderá bloquear o acesso a esses sítios.

Art. 18. A política de acesso a portais de *internet* deve ser a mesma em toda a Justiça Federal em Pernambuco.

Art. 19. Os pedidos de acesso a portais de *internet* vedados devem ser formulados à Comissão Local de Segurança da Informação.

§ 1º Fica dispensada a solicitação para magistrado ou pessoa por ele designada para fins de instrução processual.

§ 2º Dispensa-se, de igual forma, a solicitação para autoridade processante com objetivo de instruir processos administrativos, bem como para as equipes de Tecnologia da Informação responsáveis por manter o acesso à *internet*.

UTILIZAÇÃO DE CORREIO ELETRÔNICO

Art. 20. O correio eletrônico constitui recurso corporativo para comunicação e deve ser usado de modo compatível com o exercício da atividade institucional, sem comprometer a imagem da Justiça Federal em Pernambuco nem o tráfego de dados na rede de computadores da instituição.

§ 1º Todas as mensagens eletrônicas enviadas e recebidas nos domínios da Justiça Federal em Pernambuco terão registrados os dados: data e hora do envio ou recebimento, remetente e destinatário, pelo período mínimo de 5 anos.

§ 2º A área de Tecnologia da Informação deverá implantar mecanismos que evitem o envio e a recepção de mensagens que possam comprometer a segurança do serviço.

§ 3º A área de Tecnologia da Informação poderá estabelecer cotas para limitar o espaço de armazenamento das caixas postais, por unidade e/ou usuário.

§ 4º A área de Tecnologia da Informação não acessará mensagens individuais de caixas de e-mail, salvo para atender aos seguintes objetivos:

I - Verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização do Presidente do Tribunal ou do Diretor do Foro da Seção Judiciária.

II - Recuperar conteúdo de interesse da Justiça Federal, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização do Presidente do Tribunal ou do Diretor do Foro da Seção Judiciária.

III - Atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização do Diretor do Foro â€‹.

IV - Atender à determinação judicial.

V - Realizar a recuperação de mensagens do *backup*, a pedido do usuário.

Art. 21. É vedada a prática das seguintes ações relativas ao correio eletrônico:

I - Acesso ou tentativa de acesso à caixa postal em desacordo com o previsto no § 4º do artigo 20 desta Portaria.

II - Envio ou armazenamento de mensagem de conteúdo incompatível com as atribuições dos usuários, incluindo as que contêm ofensas e comentários discriminatórios.

III - Adulteração de dados referentes à origem da mensagem nos campos de controle de cabeçalho.

Parágrafo único. Para os fins deste artigo, considera-se armazenada a mensagem aberta e mantida na caixa postal.

SISTEMA DE ARQUIVOS

Art. 22. O sistema de arquivos constitui recurso corporativo, e deve ser usado de modo compatível com o exercício do cargo para armazenamento de arquivos.

Art. 23. A área de Tecnologia da Informação deverá realizar cópias de segurança (*backup*) do sistema de arquivos, conforme estipulado na Política de Cópias de Segurança.

Parágrafo único. O *backup* dos arquivos de pastas de usuário armazenadas localmente no microcomputador ou na máquina virtual, bem como de configurações personalizadas, é de responsabilidade do usuário.

Art. 24. A área de Tecnologia da Informação poderá estabelecer cotas para limitar o espaço de armazenamento das pastas, por unidade e/ou usuário.

Art. 25. A área de Tecnologia da Informação não acessará os arquivos armazenados nas pastas das unidades e dos usuários, salvo para atender aos seguintes objetivos:

I - Verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização do Diretor do Foro.

II - Recuperar conteúdo de interesse da Justiça Federal em Pernambuco, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização do Diretor do.

III - Atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização do Diretor do Foro.

IV - Atender à determinação judicial.

V - Realizar a recuperação de arquivos do *backup*, a pedido do usuário.

VI - Verificar, de forma automatizada, existência de vírus eletrônicos.

MENSAGERIA INSTANTÂNEA

Art. 26. O sistema de mensageria instantânea constitui recurso corporativo para comunicação, a ser usado de modo compatível com o exercício do cargo, sem comprometer a imagem da Justiça Federal em Pernambuco nem o tráfego de dados na rede de computadores da instituição.

§ 1º A área de Tecnologia da Informação não acessará mensagens individuais, salvo para atender aos seguintes objetivos:

I - Verificar a obtenção, retenção, uso e divulgação de informações por meio ou com fins ilícitos, ou em desacordo com as normas regulamentares sobre segurança da informação, mediante autorização do Diretor do Foro.

II - Recuperar conteúdo de interesse da Justiça Federal, no caso de afastamentos legais do usuário e de seu substituto, mediante autorização do Presidente do Diretor do Foro.

III - Atender à demanda formulada no âmbito de processo administrativo disciplinar, mediante autorização do Diretor do Foroâ€‹.

IV - Atender à determinação judicial.

V - Realizar a recuperação de mensagens do *backup*, a pedido do usuário.

VI - Verificar, de forma automatizada, a existência de vírus eletrônicos.

§ 2º A área de Tecnologia da Informação poderá manter registros de *login* de usuário e de envio de mensagens pelo sistema de mensageria instantânea.

§ 3º A ferramenta de mensageria instantânea adotada pela Seção Judiciária de Pernambuco é o TEAMS. A utilização ou conexão com sistemas de mensageria instantânea de uso público, como Windows Live Messenger, Yahoo! Messenger, Google Talk, Skype, WhatsApp, Pandion (Psi), entre outros, poderão ser restringidas a critério da Comissão Local de Segurança da Informação.[ARB1]

VIDEOCONFERÊNCIA E WEBCONFERÊCIA

Art. 27. O sistema de conferência ou reunião audiovisual à distância constitui recurso corporativo para comunicação, e deve ser usado de modo compatível com o exercício do cargo, sem comprometer a imagem da Justiça Federal em Pernambuco nem o tráfego de dados na rede de computadores da instituição.

Parágrafo único. A utilização ou conexão com sistemas de conferências de uso público, como Zoom, Cisco Webex, Microsoft Teams, entre outros, poderá ser restringida a critério da Comissão Local de Segurança da Informação.

CONTROLE DE ACESSO FÍSICO E AMBIENTAL

Art. 28. Devem ser utilizados perímetros físicos de segurança (barreiras tais como paredes e portões de entrada controlados) para proteger as áreas que contenham instalações de processamento, armazenamento e comutação de dados além de controles para minimizar o risco de ameaças físicas potenciais, tais como furto, incêndio, explosivos, fumaça, água, poeira, vibração, efeitos químicos, interferências com o suprimento de energia elétrica, interferência nas comunicações, radiação eletromagnética e vandalismo.

§ 1º Os perímetros de segurança devem ser claramente definidos e sua localização e a capacidade de resistência dos mesmos devem depender dos requisitos de segurança dos ativos existentes no interior do perímetro.

§ 2º A área de tecnologia da informação deverá avaliar e providenciar constantemente, com o auxílio das áreas competentes, a melhoria dos recursos de segurança de seus centros de processamento, armazenamento e comutação de dados corporativos.

§ 3º As áreas de processamento, armazenamento e comutação de dados devem ser protegidas por controles apropriados de entrada, para assegurar que somente pessoas autorizadas tenham acesso.

DISPOSIÇÕES FINAIS

Art. 27. Esta norma deverá ser revisada periodicamente pelo Comitê Local de Segurança da Informação com vistas a adequar a mesma às necessidades atuais.

Art. 28. [ARB2] O acontecimento de fatos supervenientes, relevantes para a segurança da informação, autorizam o Comitê Local de Segurança da Informação a rever esta política a qualquer tempo.

[ARB1]Pode ser retirado ?

[ARB2]Retirar [ARB2]

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

Documento assinado eletronicamente por **CLAUDIO KITNER**, **DIRETOR DO FORO**, em 22/03/2022, às 17:22, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.trf5.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo= informando o código verificador **2646401** e o código CRC **1501EFDA**.

Digite aqui o conteúdo do(s) anexo(s) ....